Report di Analisi: Raccolta e Monitoraggio Log con Splunk Enterprise

Questo report illustra le attività svolte per la configurazione di Splunk Enterprise, l'importazione dei dati dai log di eventi di Windows e l'analisi degli eventi di sicurezza raccolti. L'obiettivo è stato quello di configurare correttamente una pipeline di monitoraggio degli eventi e fornire una panoramica dei principali dati ottenuti.

1. Configurazione dell'ambiente Splunk

Splunk è stato installato in locale ed è stato configurato per ascoltare sulla porta predefinita 8000. L'accesso è avvenuto tramite browser, come mostrato nella prima immagine (Figura 1). La configurazione è stata eseguita in un ambiente virtualizzato tramite Oracle VirtualBox, utilizzando una macchina Windows 10 Debloated.

2. Aggiunta dei dati e configurazione input

È stato selezionato il metodo di input per i log di eventi locali (Windows Event Logs). Nella Figura 2, possiamo osservare l'interfaccia che consente di scegliere i canali di log da monitorare. In questo caso, è stato selezionato il canale di sicurezza, che contiene informazioni rilevanti su login, tentativi di accesso falliti e attività di sistema.

Nella schermata successiva (Figura 3), sono state impostate le informazioni di input: l'host è stato nominato 'splank-server' e i dati sono stati indicizzati nell'indice di default. Una volta completata la configurazione, è stata confermata la creazione dell'input per i log eventi locali (Figura 4).

3. Analisi dei log

Dopo aver completato la configurazione, è stato possibile effettuare una ricerca all'interno degli eventi raccolti (Figura 5). Sono stati rilevati 2.297 eventi di sicurezza, tutti appartenenti al tipo di sorgente 'WinEventLog:Security' (Figura 6).

Analizzando i campi, si osservano tre valori distinti per il campo 'ComputerName' (Figura 7):
- DESKTOP-8CAJRTO: 2.091 eventi (91%)
- WIN-55L622JBHP6: 194 eventi (8%)
- splank-server: 12 eventi (0,5%)

Gli eventi analizzati (Figura 8 e Figura 9) includono codici evento significativi come:
- EventCode 4672: 'Special privileges assigned to new logon', utile per identificare accessi

con privilegi elevati.
- EventCode 4624: 'An account was successfully logged on', che indica autenticazioni riuscite.

4. Conclusioni

La configurazione di Splunk ha permesso di centralizzare e analizzare i log di sicurezza generati dal sistema Windows. L'identificazione dei codici evento 4672 e 4624 consente di avere visibilità su attività critiche e login effettuati. Il sistema è ora pronto per essere utilizzato per monitoraggi in tempo reale, creazione di dashboard e generazione di alert di sicurezza.

5. Screenshot dell'analisi

Le immagini seguenti mostrano passo passo la configurazione di Splunk, l'aggiunta dei dati e i risultati delle analisi eseguite.

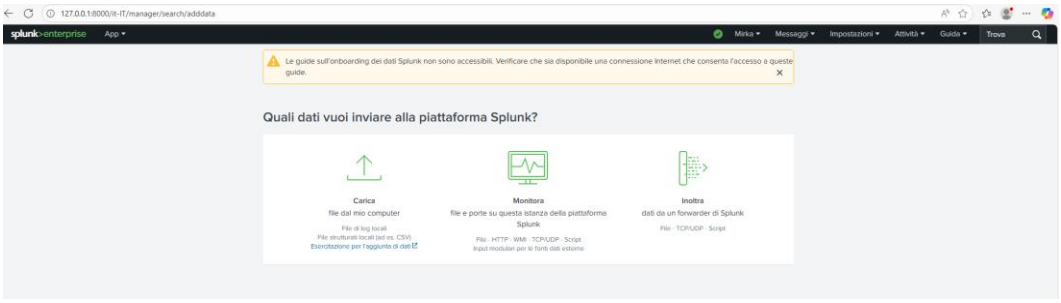

Figura 1: Interfaccia iniziale di Splunk Enterprise per l'aggiunta dati.

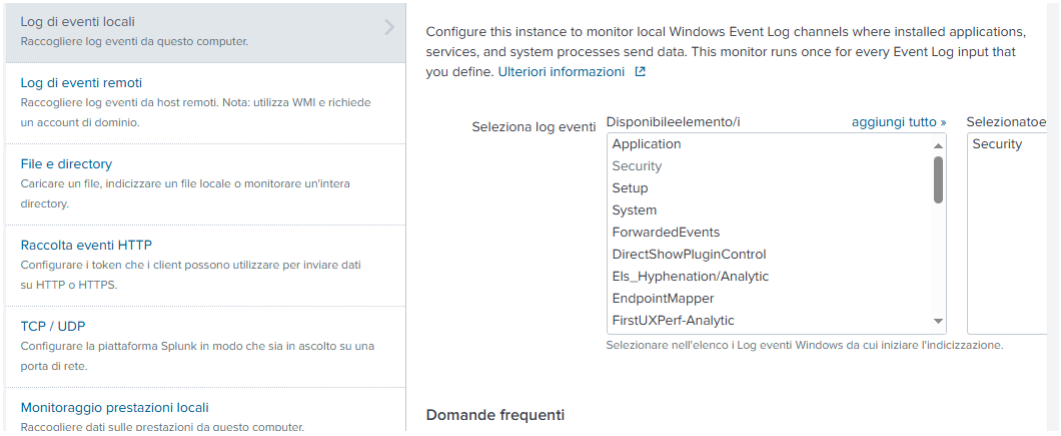

Figura 2: Scelta dei log di eventi locali di Windows.

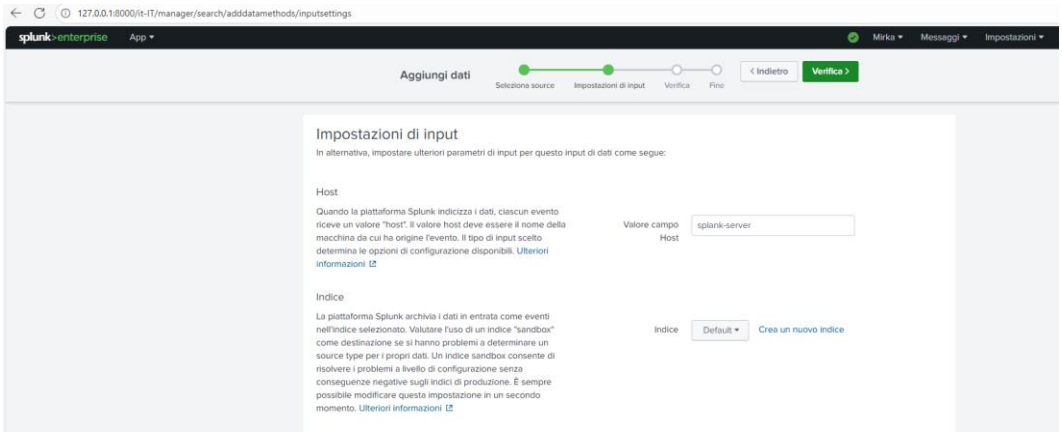

Figura 3: Impostazioni di input per host e indice.

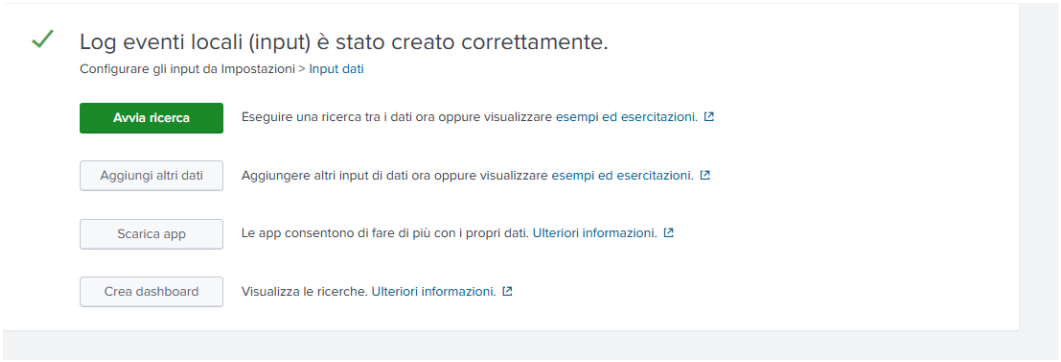

Figura 4: Conferma creazione input per log eventi locali.

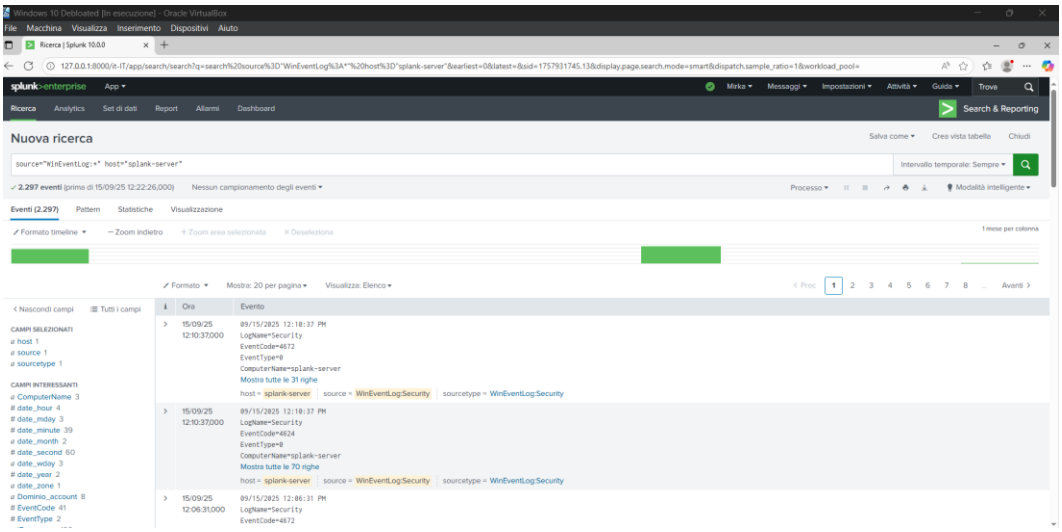

Figura 5: Ricerca eventi raccolti con Splunk.

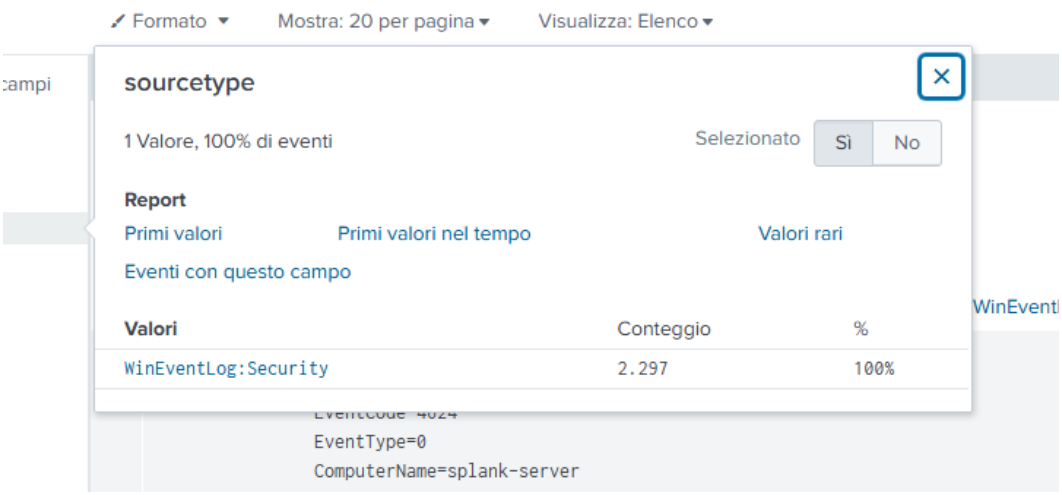

Figura 6: Tipologia di sorgente evento 'WinEventLog:Security'.

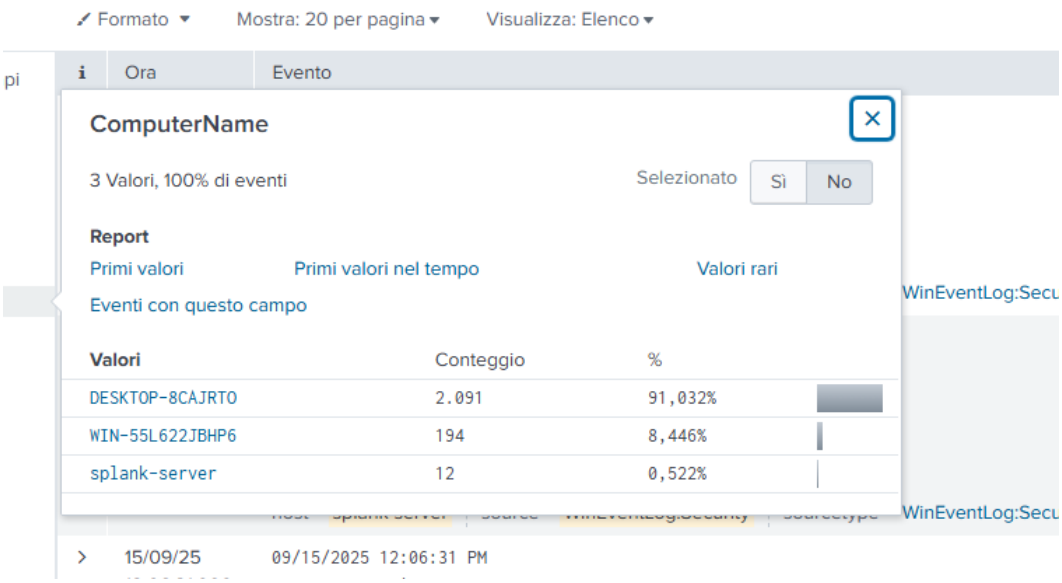

Figura 7: Analisi del campo ComputerName.

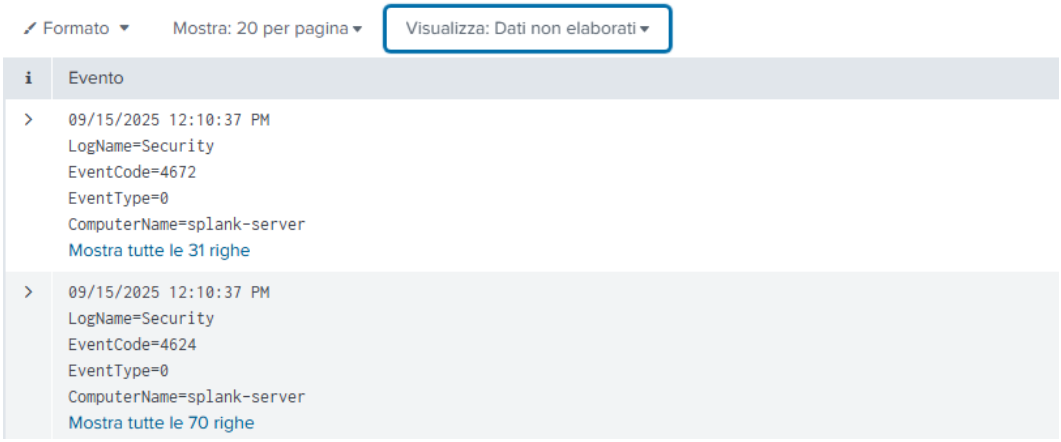

Figura 8: Visualizzazione eventi grezzi.

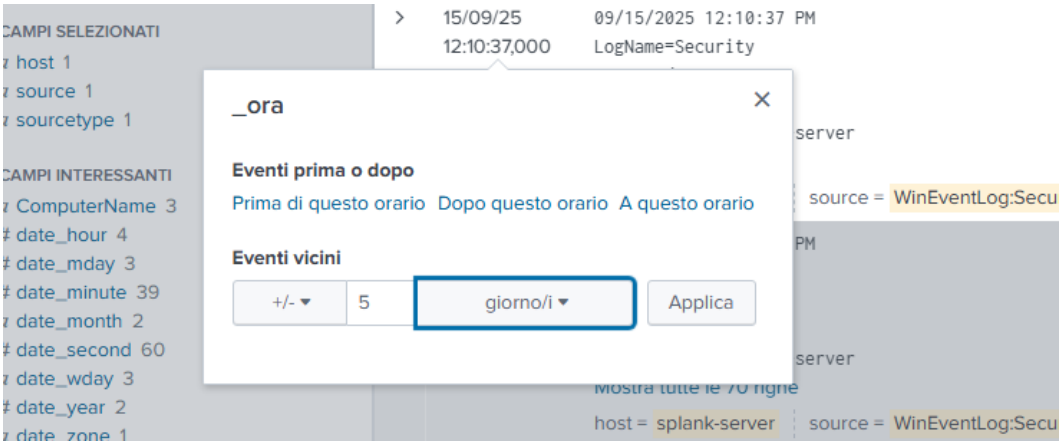

Figura 9: Filtri temporali sugli eventi.

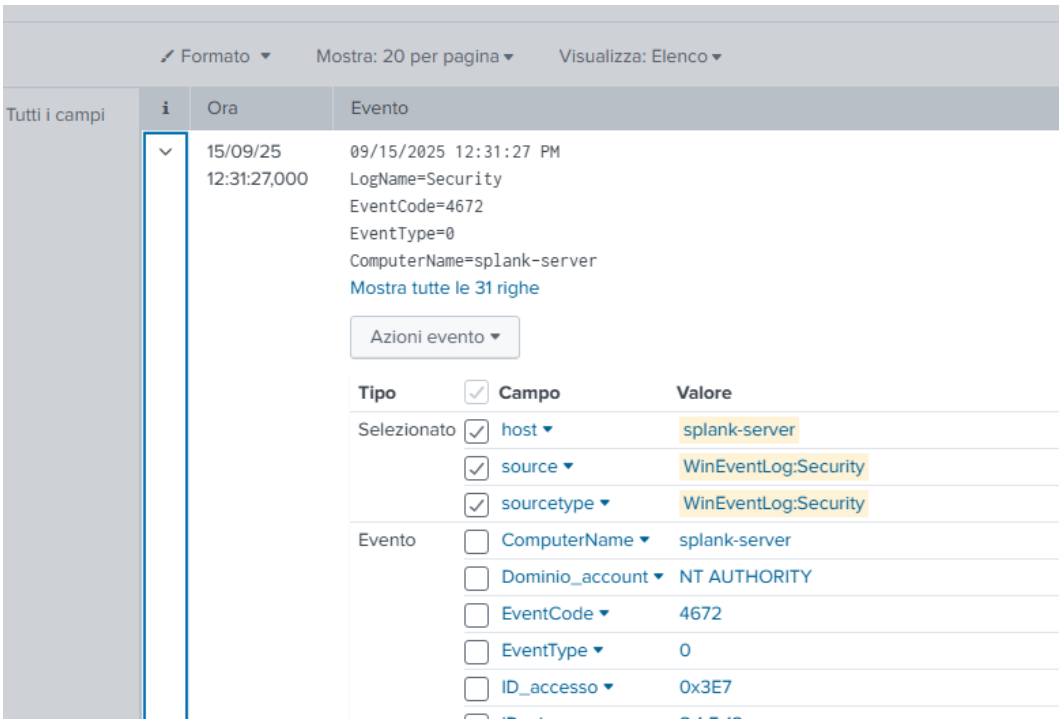

Figura 10: Dettaglio evento con codice 4672.