

REPORT TECNICO

“Monitora” Splunk

Redatto da: Nicolò Calì Cybersecurity Student

Data: 09/02/2026

Oggetto: esplorazione della funzionalità "Monitora" di Splunk

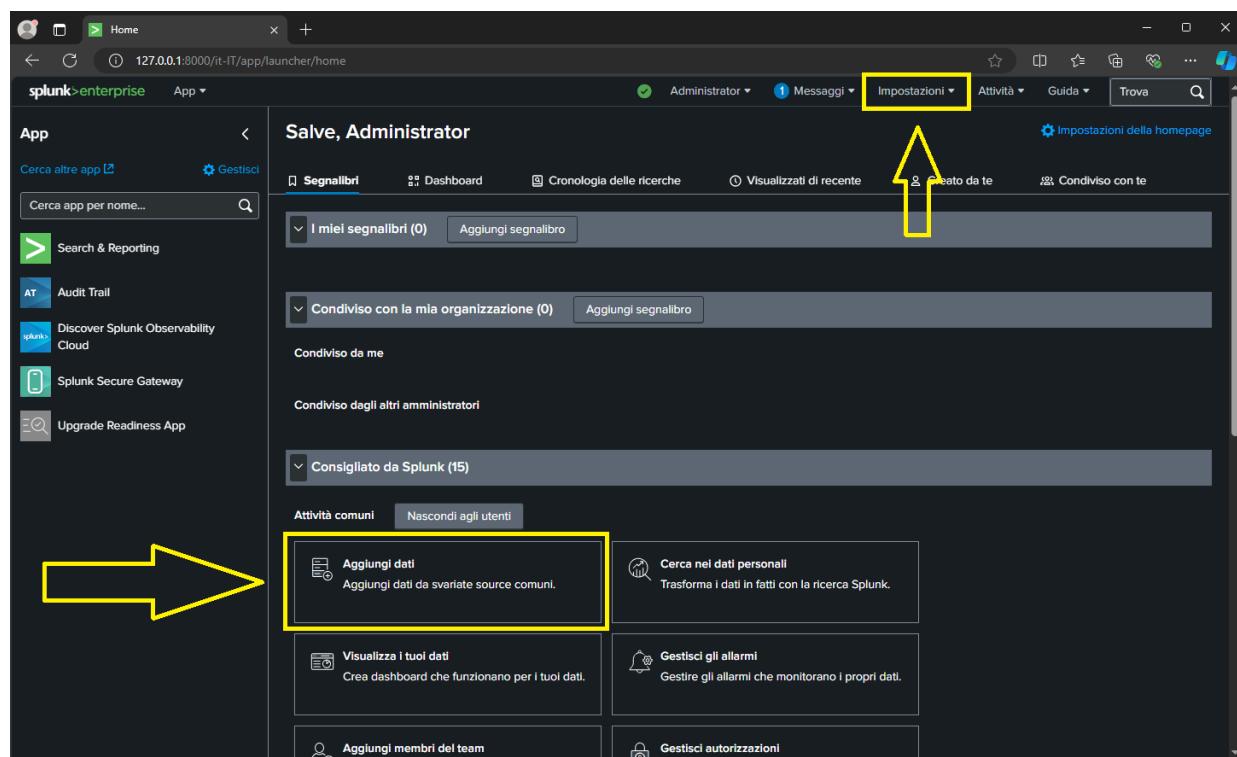
1. Introduzione

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

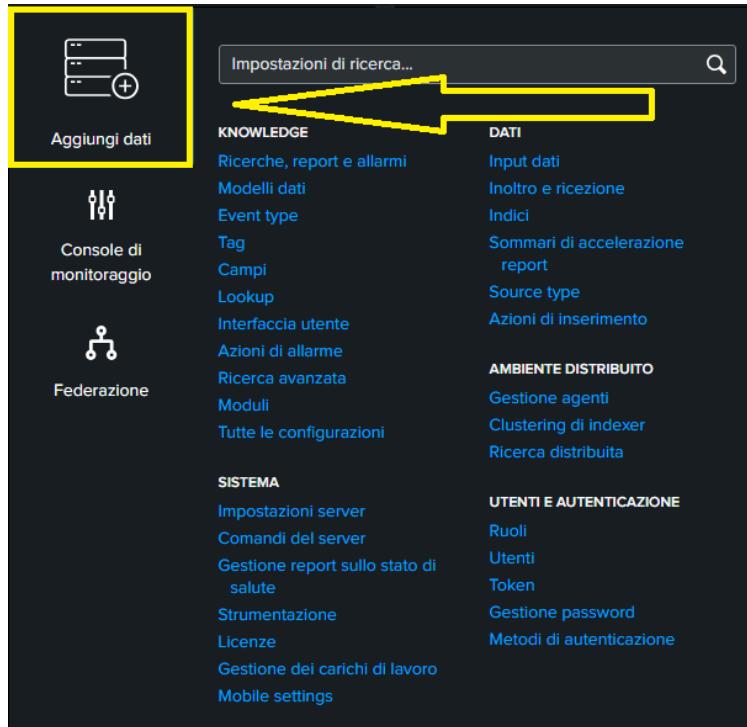
L'esercitazione è stata condotta su una workstation dotata di sistema operativo **Windows 10**. Il software utilizzato è **Splunk Enterprise**, installato localmente e configurato con le impostazioni di default. L'interazione con la piattaforma avviene tramite l'interfaccia web accessibile via browser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

Oppure, inserisci i dati utilizzando uno dei seguenti metodi

The screenshot shows the 'Add Data' page. It has three main options: 'Carica' (Upload) with a file icon, 'Monitora' (Monitor) with a graph icon, and 'Inoltra' (Forward) with a network icon. The 'Monitora' option is highlighted with a yellow box. Below it, text reads: 'file e porte su questa istanza della piattaforma Splunk', 'File - HTTP - WMI - TCP/UDP - Script', and 'Input modulari per le fonti dati esterne'.

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**

Log di eventi locali
Raccolgono log eventi da questo computer.

Log di eventi remoti
Raccolgono log eventi da host remoti. Nota: utilizza WMI e richiede un account di dominio.

File e directory
Caricare un file, indicizzare un file locale o monitorare un'intera directory.

Raccolta eventi HTTP
Configurare i token che i client possono utilizzare per inviare dati su HTTP o HTTPS.

TCP / UDP
Configurare la piattaforma Splunk in modo che sia in ascolto su una porta di rete.

Monitoraggio prestazioni locali
Raccolgono dati sulle prestazioni da questo computer.

Monitoraggio prestazioni remoto
Raccolgono informazioni su prestazioni ed eventi di host remoti. Sono necessarie le credenziali di dominio.

Monitoraggio registro di sistema
Utilizzare la piattaforma Splunk per indicizzare il registro di sistema di Windows locale e per rilevare la presenza di eventuali modifiche.

Monitoraggio di Active Directory
Individuare e monitorare Active Directory.

Selezione log eventi

Disponibile elemento/i	aggiungi tutto »	Selezionato
Application		
Security		
Setup		
System		
ForwardedEvents		
DirectShowPluginControl		
Els_Hyphenation/Analytic		
EndpointMapper		
FirstUXPerf-Analytic		

Selezionare nell'elenco i Log eventi Windows da cui iniziare l'indicizzazione.

Domande frequenti

- A quali log eventi ha accesso questa istanza della piattaforma Splunk?
- Qual è il metodo migliore per monitorare i log eventi delle macchine Windows remote?

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

Impostazioni di input

In alternativa, impostare ulteriori parametri di input per questo input di dati come segue:

Host
Quando la piattaforma Splunk indica i dati, ciascun evento riceve un valore "host". Il valore host deve essere il nome della macchina da cui ha origine l'evento. Il tipo di input scelto determina le opzioni di configurazione disponibili. Ulteriori informazioni ↗

Valore campo Host

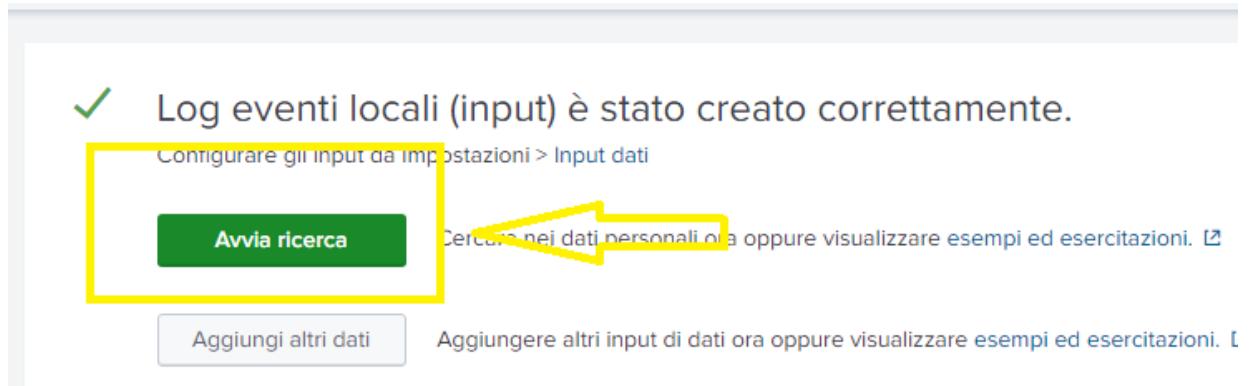
Indice
La piattaforma Splunk archivia i dati in entrata come eventi nell'indice selezionato. Valutare l'uso di un indice "sandbox" come destinazione se si hanno problemi a determinare un source type per i propri dati. Un indice sandbox consente di risolvere i problemi a livello di configurazione senza conseguenze negative sugli indici di produzione. È sempre possibile modificare questa impostazione in un secondo momento. Ulteriori informazioni ↗

Indice Crea un nuovo indice

Domande frequenti

- Come funzionano gli indici?
- Come faccio a sapere quando creare o utilizzare più indici?

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.

The screenshot shows the search results page in Splunk. A yellow box highlights the search bar containing the query "index='test_local_logs' source='WinEventLog:*'". Another yellow box highlights the search results table, which lists three events. The first event is shown in full:

Ora	Evento
09/02/26 16:06:51.231	02/09/2026 04:06:51.231 PM LogName=Security EventCode=5379 EventType=0 ComputerName=SplunkServer Mostra tutte le 21 righe host = SplunkServer source = WinEventLog:Security sourcetype = WinEventLog:Security
09/02/26 16:06:51.224	02/09/2026 04:06:51.224 PM LogName=Security EventCode=5379 EventType=0 ComputerName=SplunkServer Mostra tutte le 21 righe host = SplunkServer source = WinEventLog:Security sourcetype = WinEventLog:Security
09/02/26 16:06:51.224	02/09/2026 04:06:51.224 PM LogName=Security EventCode=5379 EventType=0 ComputerName=SplunkServer Mostra tutte le 21 righe host = SplunkServer source = WinEventLog:Security sourcetype = WinEventLog:Security

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. Conclusion 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.