

# MONITORA SPLUNK

### **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.

## Quali dati vuoi inviare alla piattaforma Splunk?

Seguire le guide sull'onboarding delle fonti di dati più popolari



### Cloud computing

Get your cloud computing data in to the Splunk platform.

10 fonti di dati



### Collegamento in rete

Immettere i dati di rete nella piattaforma Splunk.

2 fonti di dati



### Sistema operativo

Immettere i dati del sistema operativo nella piattaforma Splunk.

1 fonte di dati



### Sicurezza

Immettere i dati di sicurezza nella piattaforma Splunk.

3 fonti di dati

4 fonti di dati in totale

Oppure, inserisci i dati utilizzando uno dei seguenti metodi



### Carica

file dal mio computer

File di log locali

File strutturati locali (ad es. CSV)

[Esercitazione per l'aggiunta di dati](#)



### Monitora

file e porte su questa istanza della piattaforma Splunk

File - HTTP - WMI - TCP/UDP - Script  
Input modulari per le fonti dati esterne



### Inoltra

dati da un forwarder di Splunk

File - TCP/UDP - Script

una volta effettuato l'accesso su splunk, andiamo nella sezione aggiungi dati e successivamente su monitora

splunk>enterprise App ▾ Administrator ▾ Messaggi ▾ Impostazioni ▾ Attività ▾ Guida ▾ Trova

**Aggiungi dati**

Seleziona source    Impostazioni di input    Verifica    Fine

< Indietro    **Avanti >**

**Log di eventi locali**  
Raccogliere log eventi da questo computer.

**Log di eventi remoti**  
Raccogliere 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**  
Raccogliere dati sulle prestazioni da questo computer.

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

Configure this instance to monitor local Windows Event Log channels where installed applications, services, and system processes send data. This monitor runs once for every Event Log input that you define. [Ulteriori informazioni](#)

Seleziona log eventi

Disponibile elemento/i	aggiungi tutto >	Selezionato
Application		
<b>Security</b>		
Setup		
System		
ForwardedEvents		
Els_Hyphenation/Analytic		
EndpointMapper		
FirstUXPerf-Analytic		
AMSI/Debug		

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?

clicchiamo su log di eventi locali, selezioniamo security e  
successivamente su avanti

splunk>enterprise App ▾ Administrator ▾ Messaggi ▾ Impostazioni ▾ Attività ▾ Guida ▾ Trova

Aggiungi dati

Selezione source Impostazioni di input Verifica Fine

< Indietro Verifica >

### Impostazioni di input

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

**Host**

Quando la piattaforma Splunk indicizza 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 windows

**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 Default ▾ Crea un nuovo indice

**Domande frequenti**

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

controlliamo le impostazioni di input e clicchiamo su verifica

splunk>enterprise

App

Administrator

Messaggi

Impostazioni

Attività

Guida

Trova

### Aggiungi dati

Seleziona source   Impostazioni di input   Verifica   Fine

< Indietro   Invia >

#### Verifica

Tipo di input ..... Log eventi di Windows

Log eventi ..... Security

Contesto app ..... search

Host ..... windows

Indice ..... default

arrivati a questa schermata clicchiamo su invia

splunk>enterprise App ▾ Administrator ▾ Messaggi ▾ Impostazioni ▾ Attività ▾ Guida ▾ Trova 🔍

Aggiungi dati

Seleziona source Impostazioni di input Verifica Fine

< Indietro Avanti >

✓ Log eventi locali (input) è stato creato correttamente.  
Configurare gli input da Impostazioni > Input dati

**Avvia ricerca** Esegui una ricerca tra i dati ora oppure visualizzare esempi ed esercitazioni. [🔗](#)

Aggiungi altri dati Aggiungere altri input di dati ora oppure visualizzare esempi ed esercitazioni. [🔗](#)

Scarica app Le app consentono di fare di più con i propri dati. Ulteriori informazioni. [🔗](#)

Crea dashboard Visualizza le ricerche. Ulteriori informazioni. [🔗](#)

una volta creato il log di eventi locali correttamente avviamo la ricerca

Questa schermata ci dice che:

- Stiamo analizzando i log di sicurezza di Windows (WinEventLog:Security) provenienti da un host specifico (windows).

- Tutti gli eventi trovati appartengono al registro di sicurezza di Windows, il che è comune quando si monitora la sicurezza di un sistema Windows.

- Abbiamo 1245 eventi totali che corrispondono ai criteri di ricerca.

- I campi selezionati e interessanti offrono un'ampia gamma di informazioni utili per l'analisi della sicurezza, come l'ora e la data dell'evento, il nome del computer, e dettagli dell'account.

The screenshot displays the Splunk search results interface. The search bar at the top shows the query: `search%20source%3D%20host%3D%20windows%20&earl...`. The results are displayed in a table with columns: Tipo, Campo, Valore, and Azioni. The first row shows a 'Selezionato' (Selected) event with fields like host, source, and sourcetype. The second row shows an 'Evento' (Event) with fields like Codice\_restituito, ComputerName, Dominio\_account, EventCode, EventType, ID\_accesso, ID\_handle, ID\_processo, ID\_sicurezza, index, Keywords, linecount, LogName, Message, Nome\_account, Nome\_algorithmo, and Nome\_providers.

Tipo	Campo	Valore	Azioni
Selezionato	host	WINDOWS	
	source	WinEventLog:Security	
	sourcetype	WinEventLog:Security	
Evento	Codice_restituito	0x0	
	ComputerName	windows	
	Dominio_account	WORKGROUP	
	EventCode	5061	
	EventType	0	
	ID_accesso	0x3E7	
	ID_sicurezza	S-1-5-18	
	Keywords	Controllo riuscito	
	LogName	Security	
	Message	Operazione di crittografia. Soggetto: ID sicurezza: S-1-5-18 Nome account: WINDOWS\$ Dominio account: WORKGROUP ID accesso: 0x3E7 Parametri di crittografia: Nome provider: Microsoft Software Key Storage Provider Nome algoritmo: RSA Nome chiave: C:\Program Files\Splunk\etc\auth\server.pem.pfx Tipo di chiave: Chiave computer. Operazione di crittografia: Operazione: Apri una chiave. Codice restituito: 0x0	
	Nome_account	WINDOWS\$	
	Nome_algorithmo	RSA	
	Nome_providers	Microsoft Software Key Storage Provider	

Questa schermata mostra come Splunk può essere utilizzato per analizzare grandi quantità di dati di log di sicurezza di Windows. Utilizzando i campi selezionati e interessanti, possiamo eseguire query avanzate per ottenere insight significativi sui nostri dati di sicurezza.