Configurazione della Modalità Monitora in Splunk

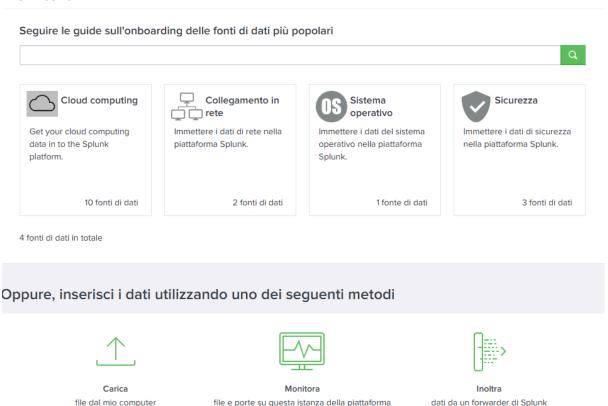
Obiettivo:

Il compito di oggi consiste nel configurare la modalità Monitora in Splunk e realizzare degli screenshot che confermino l'avvenuta configurazione.

monitora

File di log locali

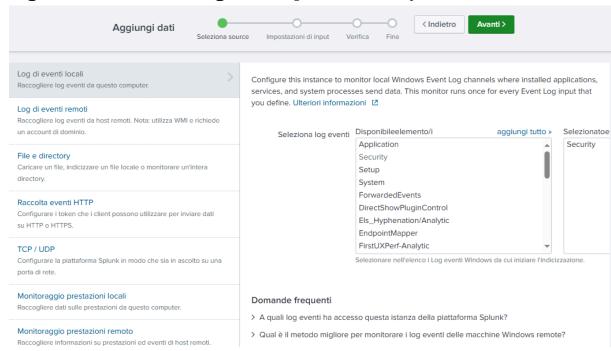
File strutturati locali (ad es. CSV) Esercitazione per l'aggiunta di dati ☑



Splunk

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

Log di eventi locali → Scegliamo l'opzione security



Avvia ricerca

✓ Log eventi locali (input) è stato creato correttamente.

Configurare gli input da Impostazioni > Input dati

