

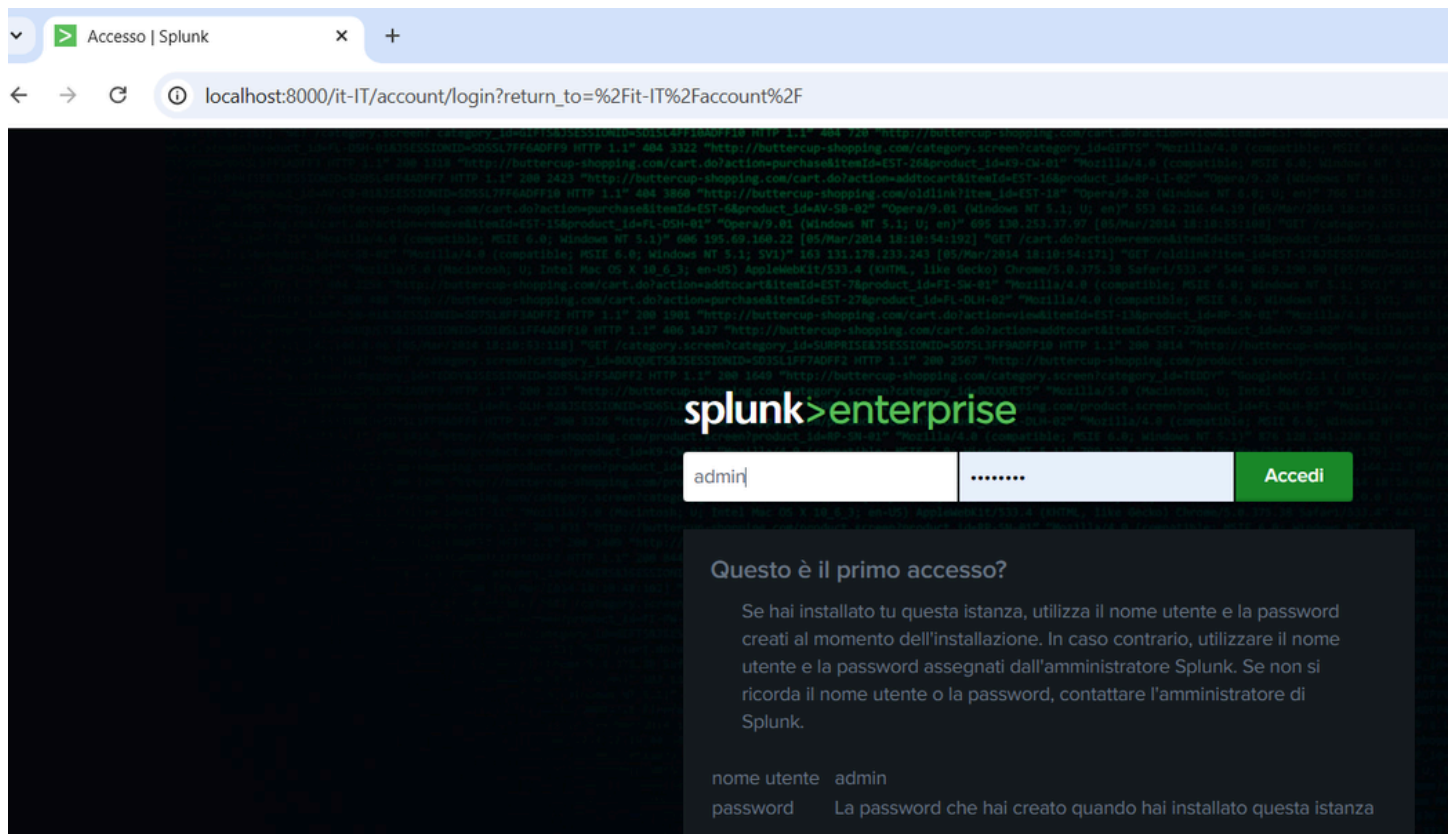
Introduzione:

L'obiettivo dell'esercizio è stato quello di esplorare e configurare la modalità **Monitora** in Splunk, una delle funzionalità fondamentali per acquisire dati in tempo reale da fonti come file, directory, e input di rete. Questa attività permette di comprendere come Splunk integri ed elabori grandi volumi di dati per generare analisi avanzate. Durante l'esercitazione, sono stati configurati i parametri di monitoraggio e verificate le operazioni tramite l'interfaccia grafica e query di ricerca.

Pratica:

Per la configurazione, si è utilizzato Splunk Enterprise accedendo alla sua interfaccia tramite browser web. Tramite l'indirizzo:

http://127.0.0.1:8000



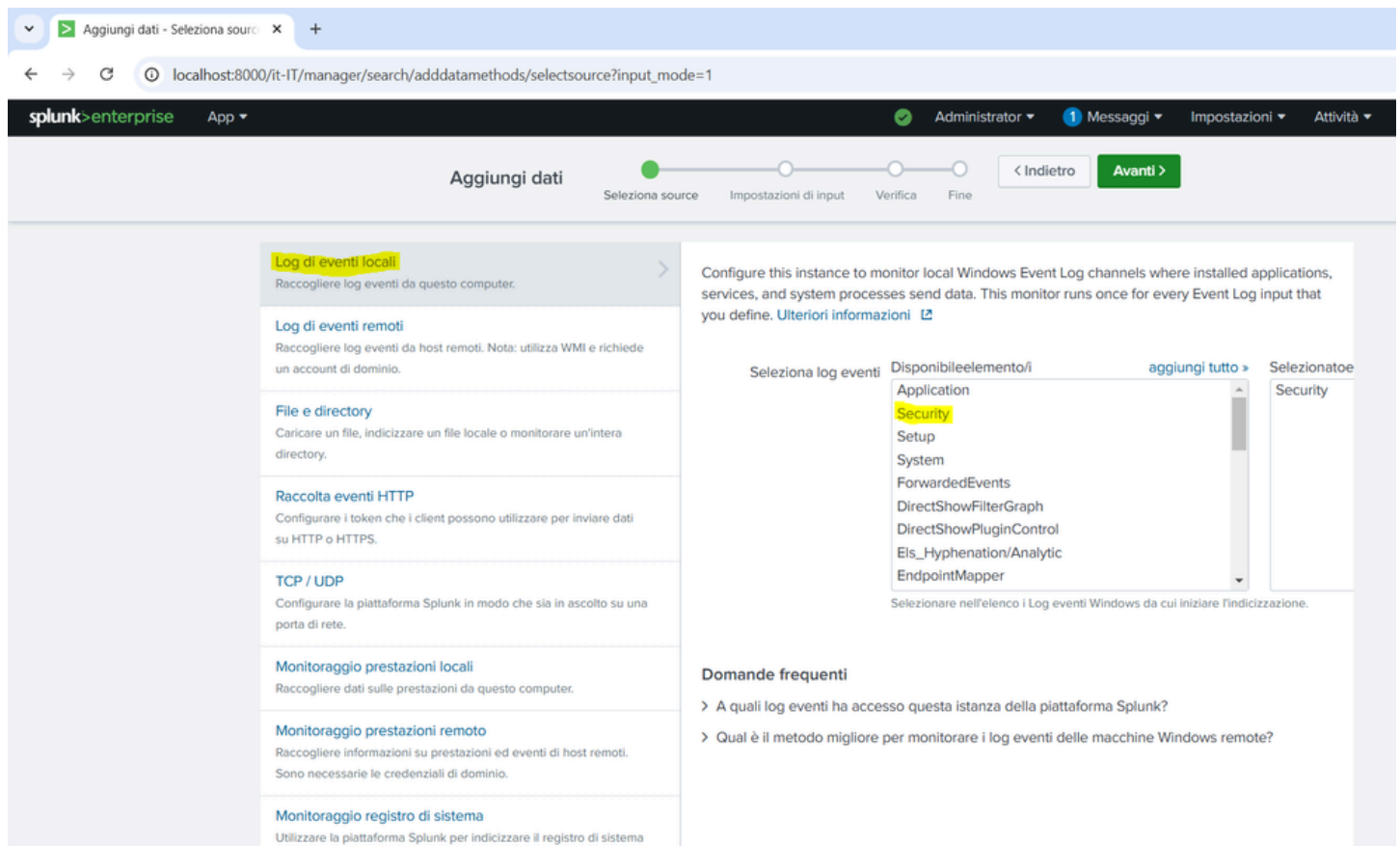
Andiamo su **impostazioni** e clicchiamo su **aggiungi dati**:

The screenshot shows the Splunk Enterprise interface. The top navigation bar includes 'splunk>enterprise', 'App', and user roles like 'Administrator'. The main dashboard area is titled 'Salve, Administrator' and contains sections for 'Segnalibri', 'Dashboard', and 'Cronologia delle ricerche'. A dropdown menu is open for the 'Aggiungi dati' button, displaying a list of data sources. The 'Monitora' option is highlighted in the dropdown.

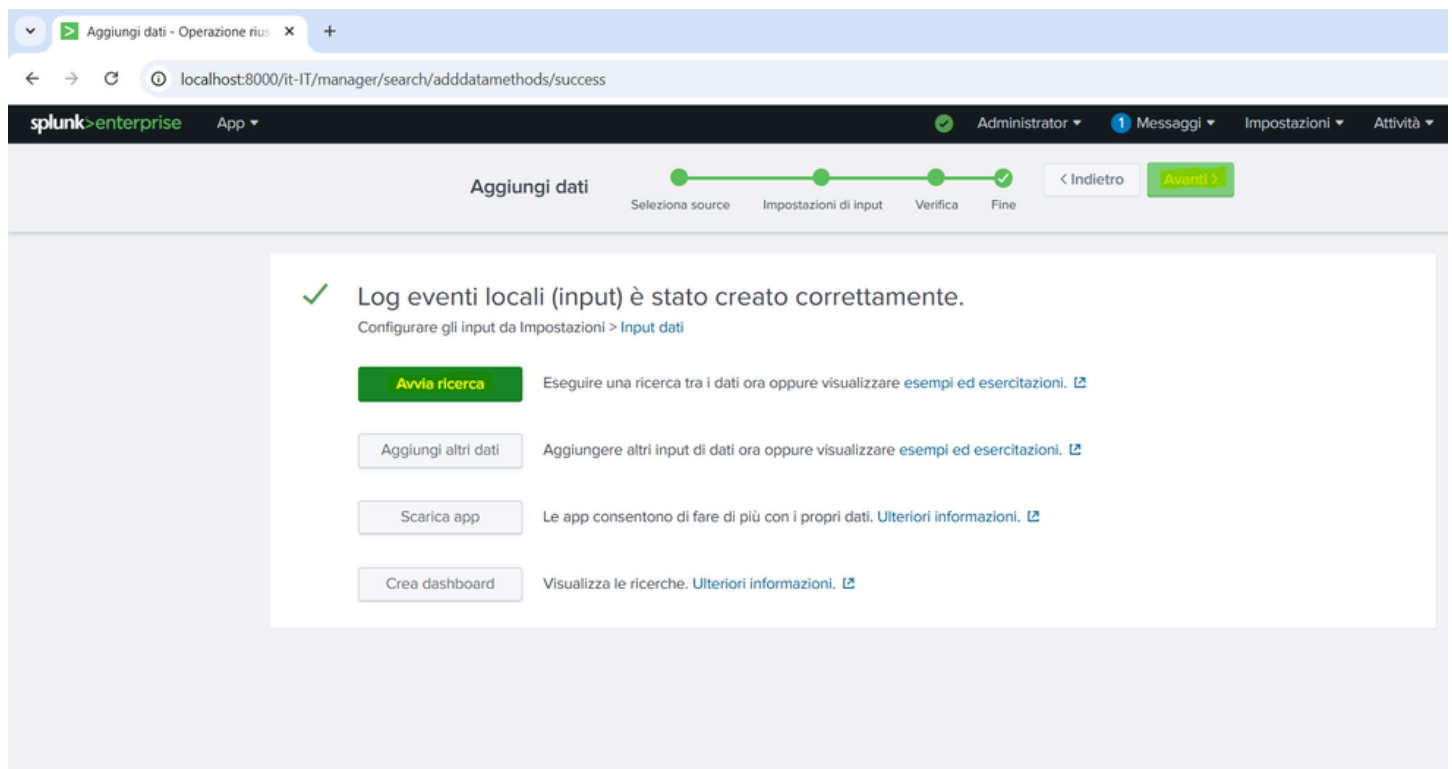
E selezioniamo la **modalità monitora**:

The screenshot shows the 'Aggiungi dati | Splunk 9.3.2' page. It features a section titled 'Seguire le guide sull'onboarding delle fonti di dati più popolari' with four cards: 'Cloud computing' (10 fonti di dati), 'Collegamento in rete' (2 fonti di dati), 'Sistema operativo' (1 fonte di dati), and 'Sicurezza' (3 fonti di dati). Below this, a section titled 'Oppure, inserisci i dati utilizzando uno dei seguenti metodi' shows three methods: 'Carica' (file dal mio computer), 'Monitora' (file e porte su questa istanza della piattaforma Splunk), and 'Inoltra' (dati da un forwarder di Splunk). The 'Monitora' method is highlighted.

Successivamente clicchiamo su **Log di eventi locali**, ed i log eventi che andremo a scegliere saranno quelli **security**:

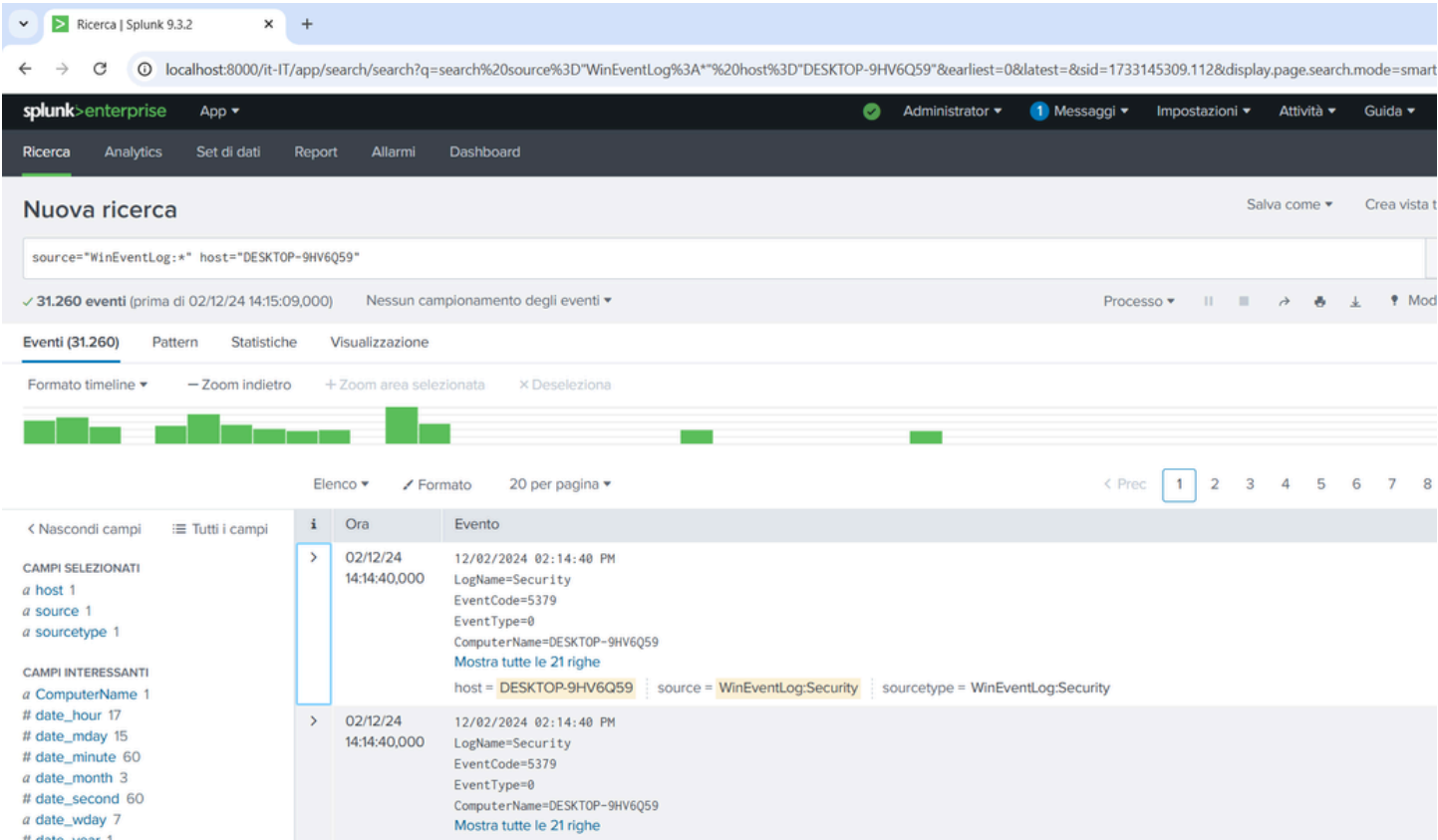


Clicchiamo **avanti** finché non arriviamo a questa schermata, dove avremmo il tasto **avvia ricerca**:

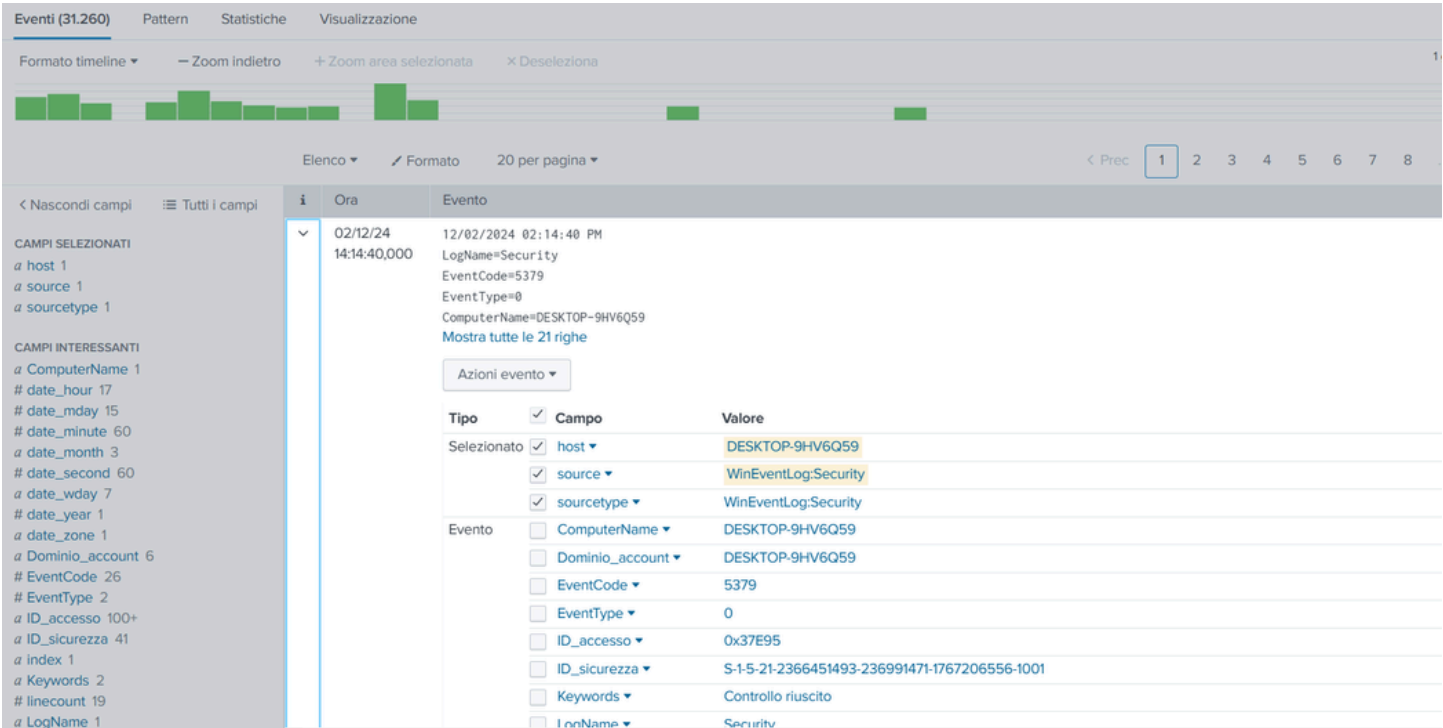


Viene mostrata quindi una ricerca relativa alla sorgente **WinEventLog** e all'host **DESKTOP-9HV6Q59**, che ha restituito **31.260 eventi**. Il grafico a barre in alto rappresenta la distribuzione temporale degli eventi, mentre l'elenco sottostante fornisce dettagli come timestamp, nome della sorgente (WinEventLog:Security) e codice evento. Sul lato

sinistro, i campi estratti automaticamente, come ComputerName ed EventCode, permettono ulteriori analisi. Questa panoramica conferma l'efficacia di Splunk nel raccogliere e organizzare i dati in modo chiaro.



Per **approfondire** un evento specifico con codice 5379. Splunk ha estratto dettagli chiave come l'host (**DESKTOP-9HV6Q59**), il dominio dell'account e il messaggio "Controllo riuscito". I campi strutturati rendono l'evento comprensibile e analizzabile, e le azioni disponibili consentono ulteriori elaborazioni come **report** o **alert**. Questa capacità dimostra la precisione di Splunk nell'analisi puntuale degli eventi.



Conclusione

L'analisi effettuata ha confermato il successo della configurazione di Splunk per monitorare i dati di sicurezza di Windows. La piattaforma ha dimostrato la sua capacità di estrarre campi rilevanti e fornire una visualizzazione intuitiva degli eventi, facilitando la comprensione dei dati acquisiti. Questa esercitazione ha rappresentato un'opportunità importante per approfondire l'utilizzo di Splunk nel contesto della gestione dei log di sicurezza e nell'analisi degli eventi, offrendo strumenti utili per individuare problemi di sistema o violazioni di sicurezza.