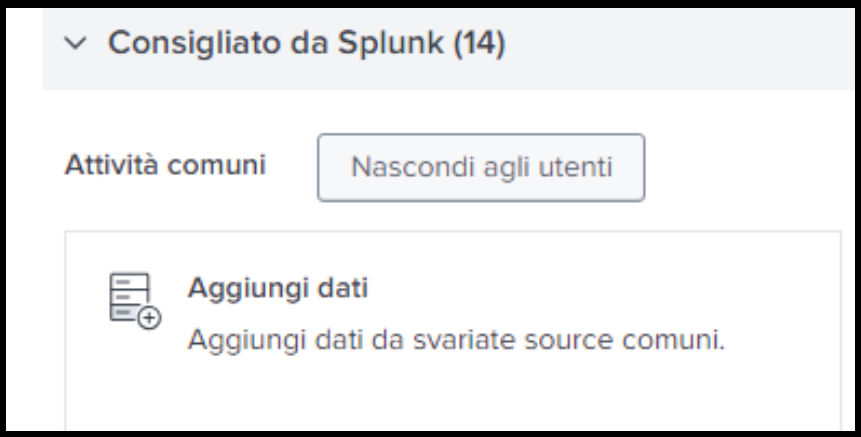
Splunk

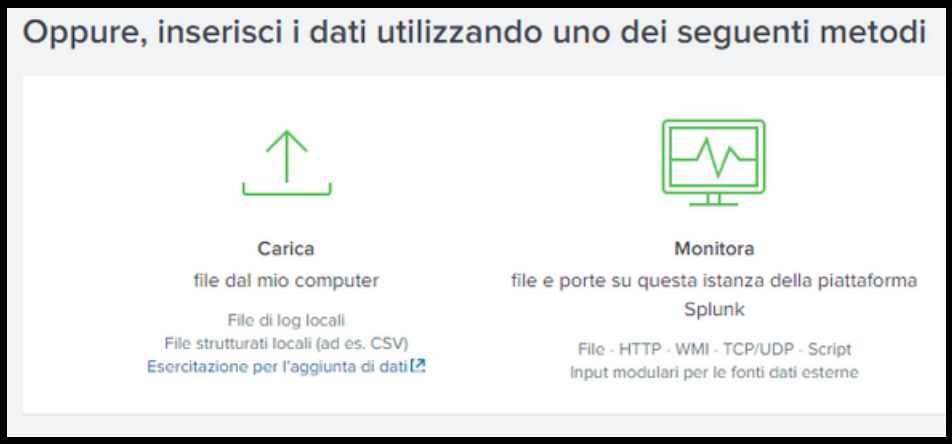
Esercizio di oggi: Configurazione della Modalità Monitora in Splunk

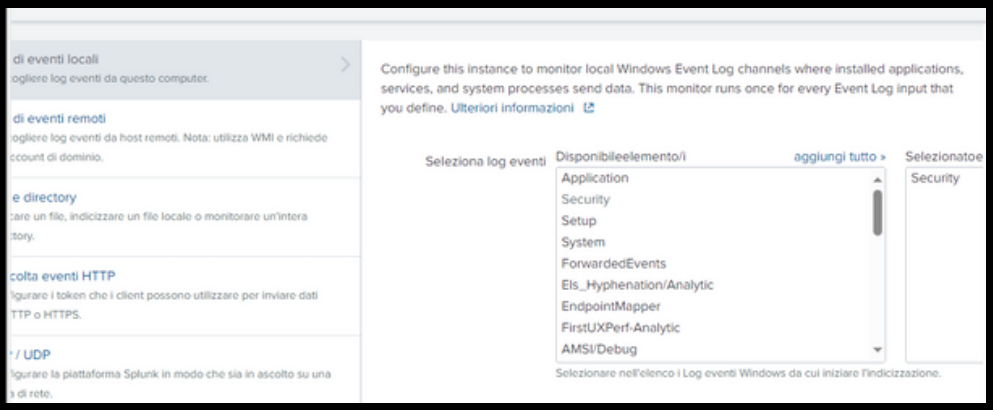
Abbiamo esplorato diverse funzionalità offerte da Splunk. Oggi ci concentreremo sulla modalità "Monitora". Il compito di oggi consiste nel configurare la modalità Monitora in Splunk e realizzare degli screenshot che confermino l'avvenuta configurazione.

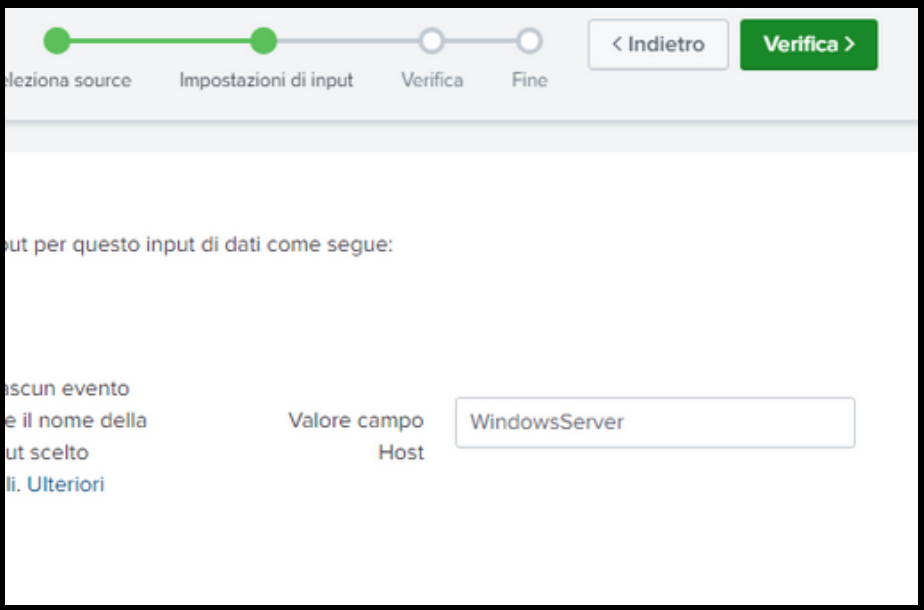
In breve: Lo studente dovrà configurare la modalità Monitora in Splunk e realizzare degli screenshot che mostrino l'esecuzione.

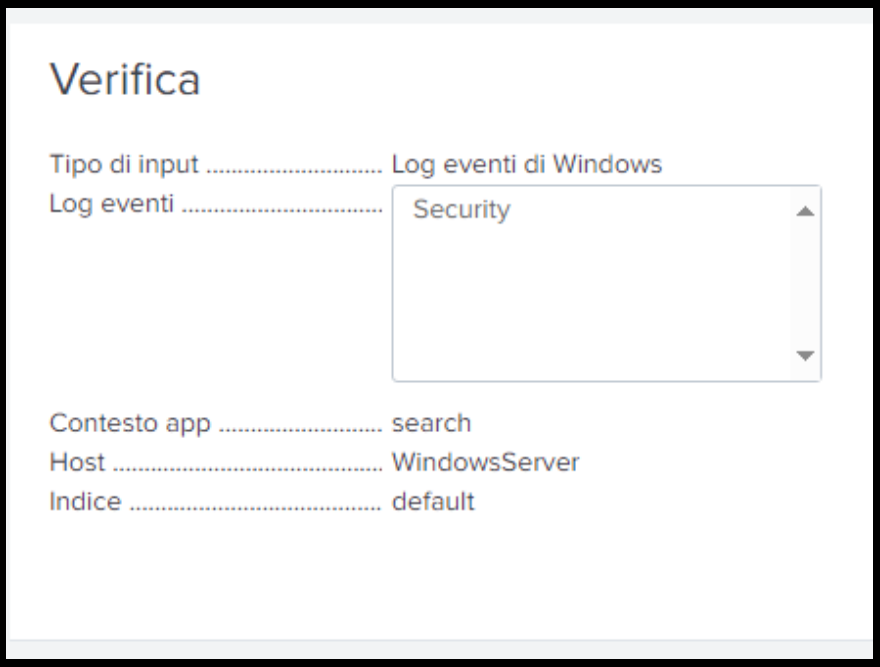
Monitora

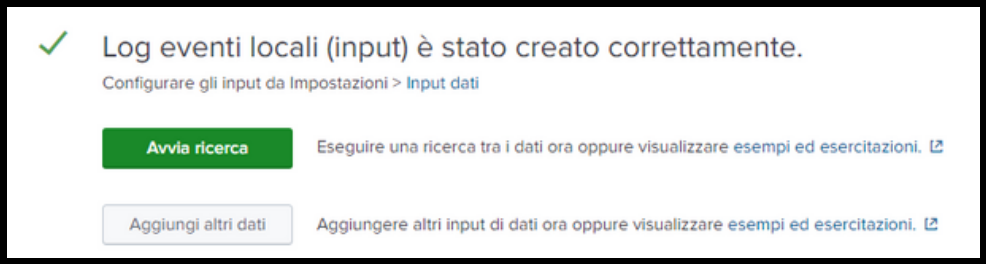

Consigliato da Splunk (14)
Attività comuni
Nascondi agli utenti
Aggiungi dati
Aggiungi dati da svariate source comuni.

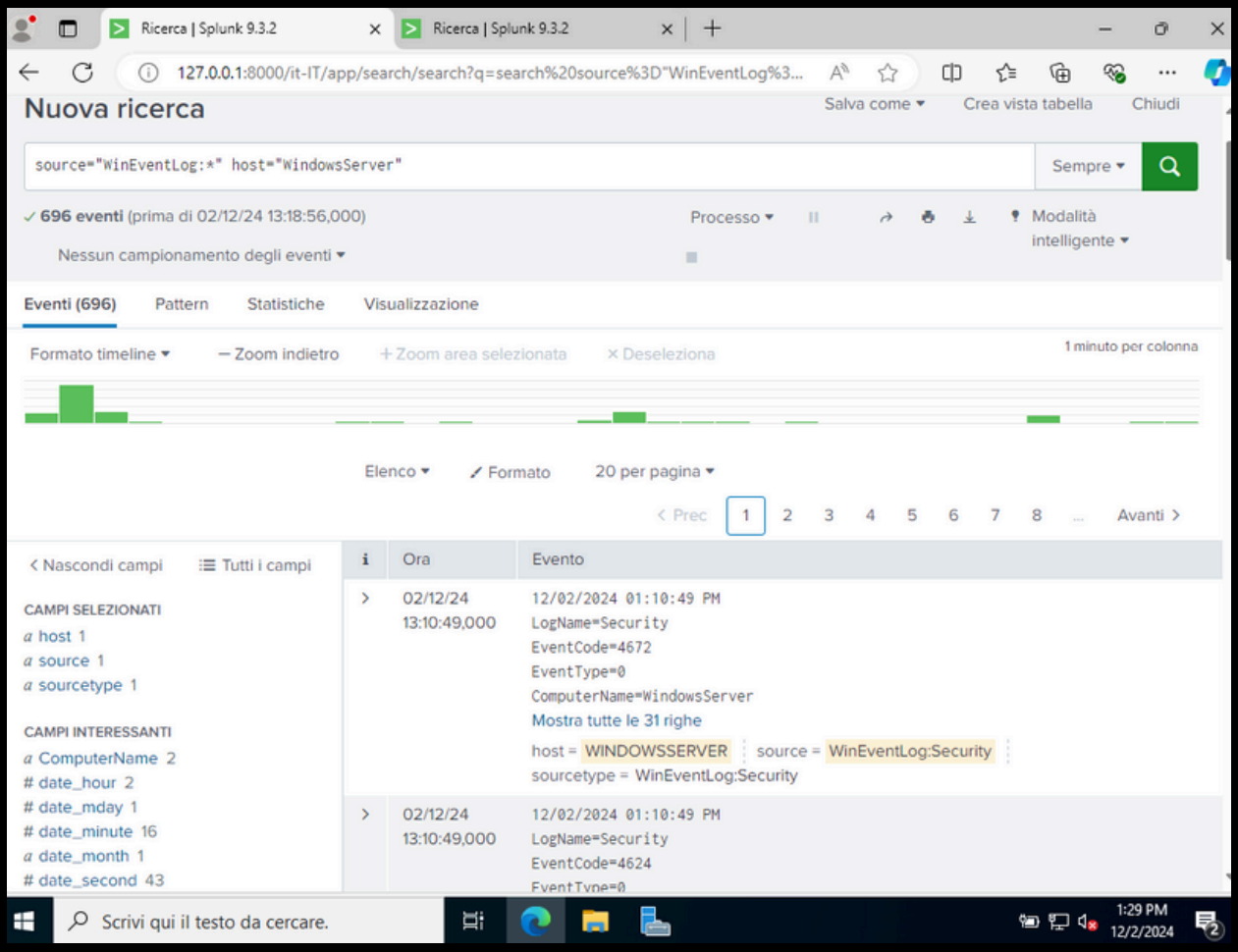

Oppure, inserisci i dati utilizzando uno dei seguenti metodi
Carica
file dal mio computer
File di log locali
File strutturati locali (ad es. CSV)
Esercitazione per l'aggiunta di dati
Monitora
file e porte su questa istanza della piattaforma Splunk
File - HTTP - WMI - TCP/UDP - Script
Input modulari per le fonti dati esterne


di eventi locali
ogliere log eventi da questo computer.
di eventi remoti
ogliere log eventi da host remoti. Nota: utilizza WMI e richiede
ccount di dominio.
e directory
are un file, indicizzare un file locale o monitorare un'intera
tory.
colta eventi HTTP
gurare i token che i client possono utilizzare per inviare dati
TTP o HTTPS.
/ UDP
gurare la piattaforma Splunk in modo che sia in ascolto su una
di rete.
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
Disponibileelemento/i
aggiungi tutto »
Selezionatoe
Application
Security
Setup
System
ForwardedEvents
Els_Hyphenation/Analytic
EndpointMapper
FirstUXPerf-Analytic
AMSI/Debug
Security
Selezionare nell'elenco i Log eventi Windows da cui iniziare l'indicizzazione.


leziona source
Impostazioni di input
Verifica
Fine
< Indietro
Verifica >
ut per questo input di dati come segue:
scun evento
e il nome della
ut scelto
li. Ulteriori
Valore campo
Host
WindowsServer

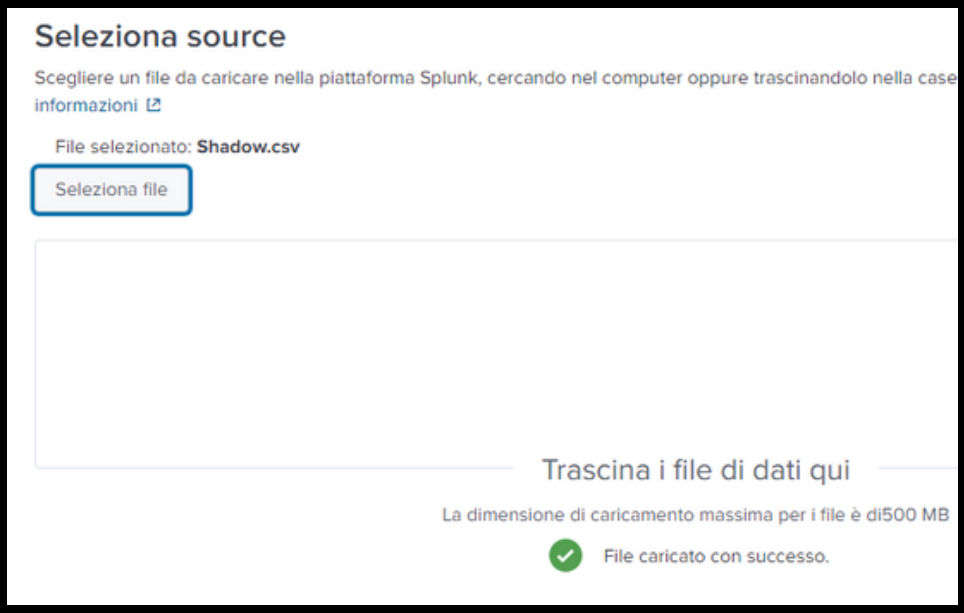

Verifica
Tipo di input ..... Log eventi di Windows
Log eventi .....
Security
Contesto app ..... search
Host ..... WindowsServer
Indice ..... default

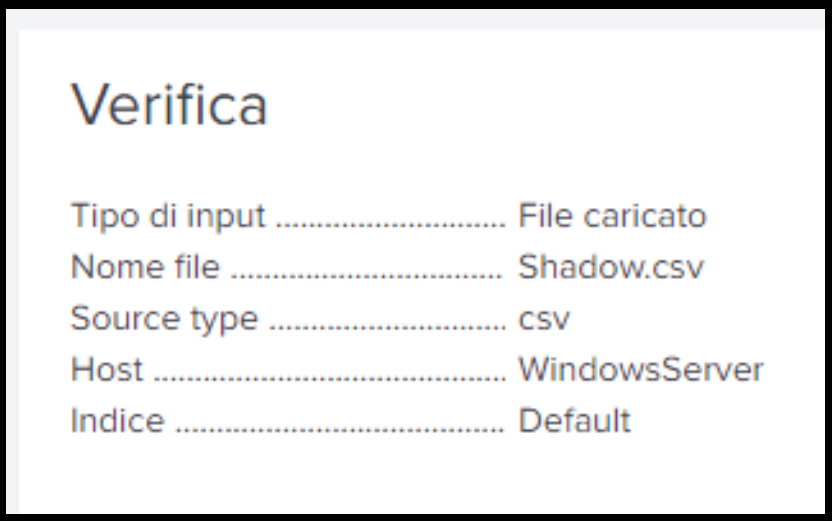

Log eventi locali (input) è stato creato correttamente.
Configurare gli input da Impostazioni > Input dati
Avvia ricerca
Eseguire una ricerca tra i dati ora oppure visualizzare esempi ed esercitazioni.
Aggiungi altri dati
Aggiungere altri input di dati ora oppure visualizzare esempi ed esercitazioni.


Ricerca | Splunk 9.3.2
127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"WinEventLog%3...
Nuova ricerca
Salva come
Crea vista tabella
Chiudi
source="WinEventLog:*" host="WindowsServer"
Sempre
696 eventi (prima di 02/12/24 13:18:56,000)
Processo
Modalità intelligente
Nessun campionamento degli eventi
Eventi (696)
Pattern
Statistiche
Visualizzazione
Formato timeline
Zoom indietro
Zoom area selezionata
Deseleziona
1 minuto per colonna
Elenco
Formato
20 per pagina
Prec
Avanti
Nascondi campi
Tutti i campi
CAMPI SELEZIONATI
host 1
source 1
sourcetype 1
CAMPI INTERESSANTI
ComputerName 2
date_hour 2
date_mday 1
date_minute 16
date_month 1
date_second 43
Ora
Evento
02/12/24 13:10:49,000
12/02/2024 01:10:49 PM
LogName=Security
EventCode=4672
EventType=0
ComputerName=WindowsServer
Mostra tutte le 31 righe
host = WINDOWSSERVER
source = WinEventLog:Security
sourcetype = WinEventLog:Security
02/12/24 13:10:49,000
12/02/2024 01:10:49 PM
LogName=Security
EventCode=4624
Scrivi qui il testo da cercare.
1:29 PM
12/2/2024

File Shadow

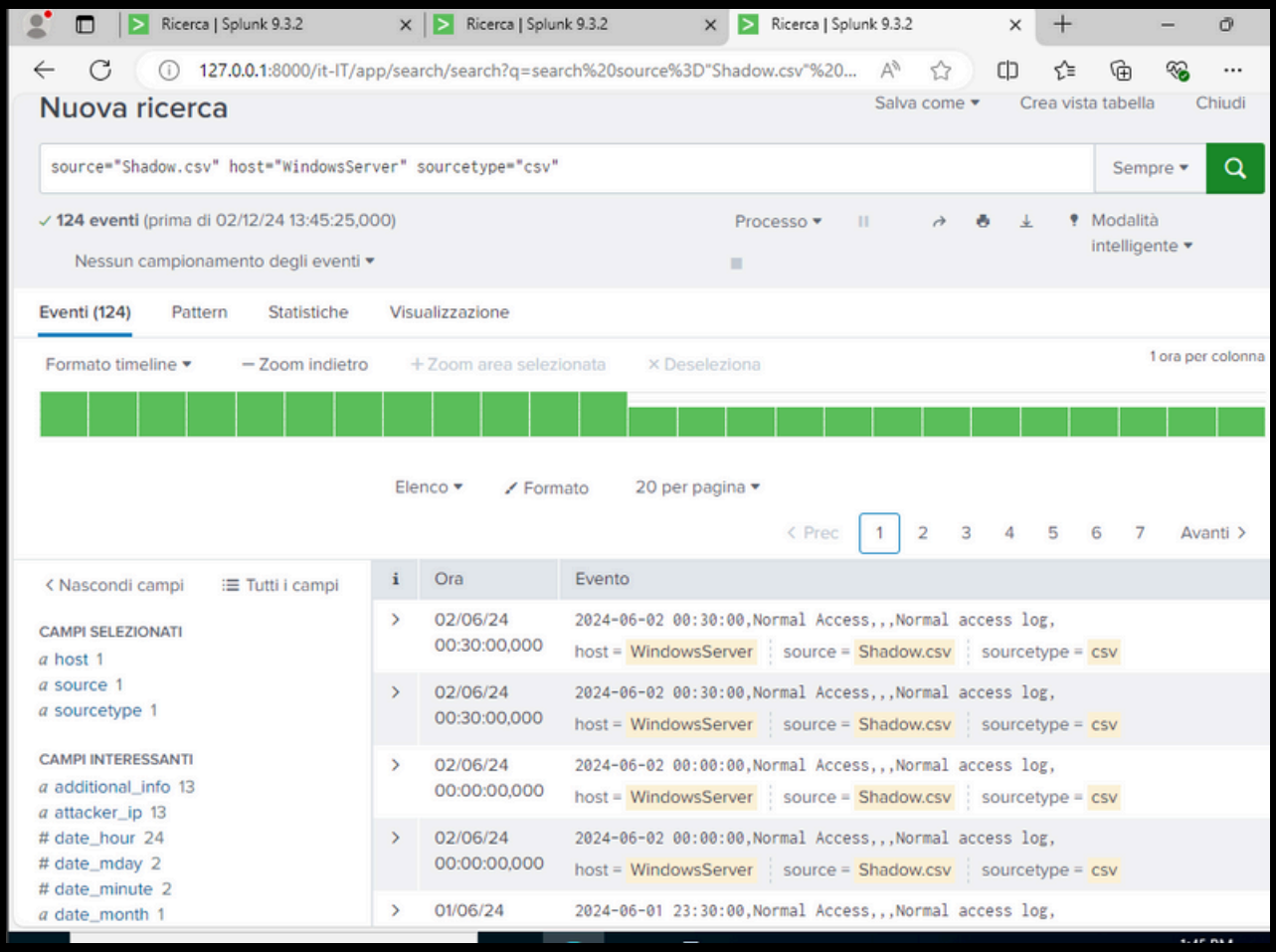

Oppure, inserisci i dati utilizzando uno dei seguenti metodi
Carica
file dal mio computer
File di log locali
File strutturati locali (ad es. CSV)
Esercitazione per l'aggiunta di dati
Monitora
file e porte su questa istanza della piattaforma Splunk
File - HTTP - WMI - TCP/UDP - Script
Input modulari per le fonti dati esterne


Seleziona source
Scegliere un file da caricare nella piattaforma Splunk, cercando nel computer oppure trascinandolo nella case
informazioni
File selezionato: Shadow.csv
Seleziona file
Trascina i file di dati qui
La dimensione di caricamento massima per i file è di500 MB
File caricato con successo.


Verifica
Tipo di input ..... File caricato
Nome file ..... Shadow.csv
Source type ..... csv
Host ..... WindowsServer
Indice ..... Default

Verifica

Tipo di input ..... File caricato
Nome file ..... Shadow.csv
Source type ..... csv
Host ..... WindowsServer
Indice ..... Default



Relazione

Splunk è una piattaforma di software progettata per raccogliere, indicizzare e analizzare grandi volumi di dati generati dai sistemi IT. In particolare, è utilizzato per monitorare e visualizzare log provenienti da server, applicazioni e dispositivi di rete, permettendo di estrarre informazioni utili per la sicurezza e l'ottimizzazione delle operazioni. Nel contesto della sicurezza informatica, Splunk è uno strumento fondamentale per identificare anomalie, monitorare eventi sospetti e generare alert in tempo reale. È particolarmente utile per analizzare i log di sicurezza di sistemi complessi, come i server Windows, dove è possibile configurare facilmente il monitoraggio e visualizzare i dati in modo intuitivo. La piattaforma offre anche funzionalità avanzate, come il machine learning, che possono essere sfruttate per migliorare le capacità di rilevamento delle minacce. Anche se può sembrare complesso, Splunk consente di iniziare con configurazioni di base, come il monitoraggio dei log di sicurezza, per poi approfondire funzionalità più avanzate in base alle esigenze.

Daniel_Gabriel_Costeanu