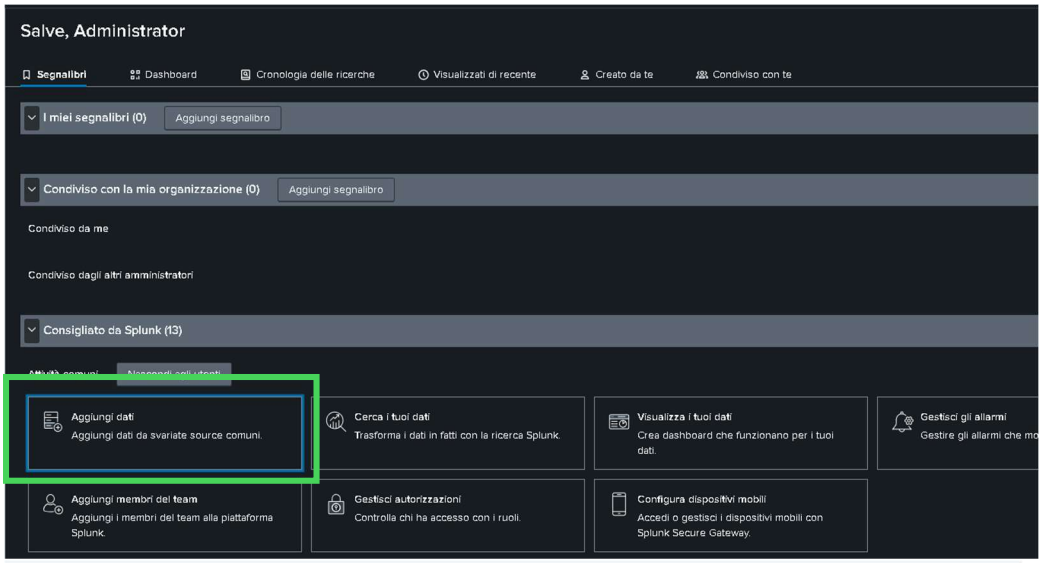
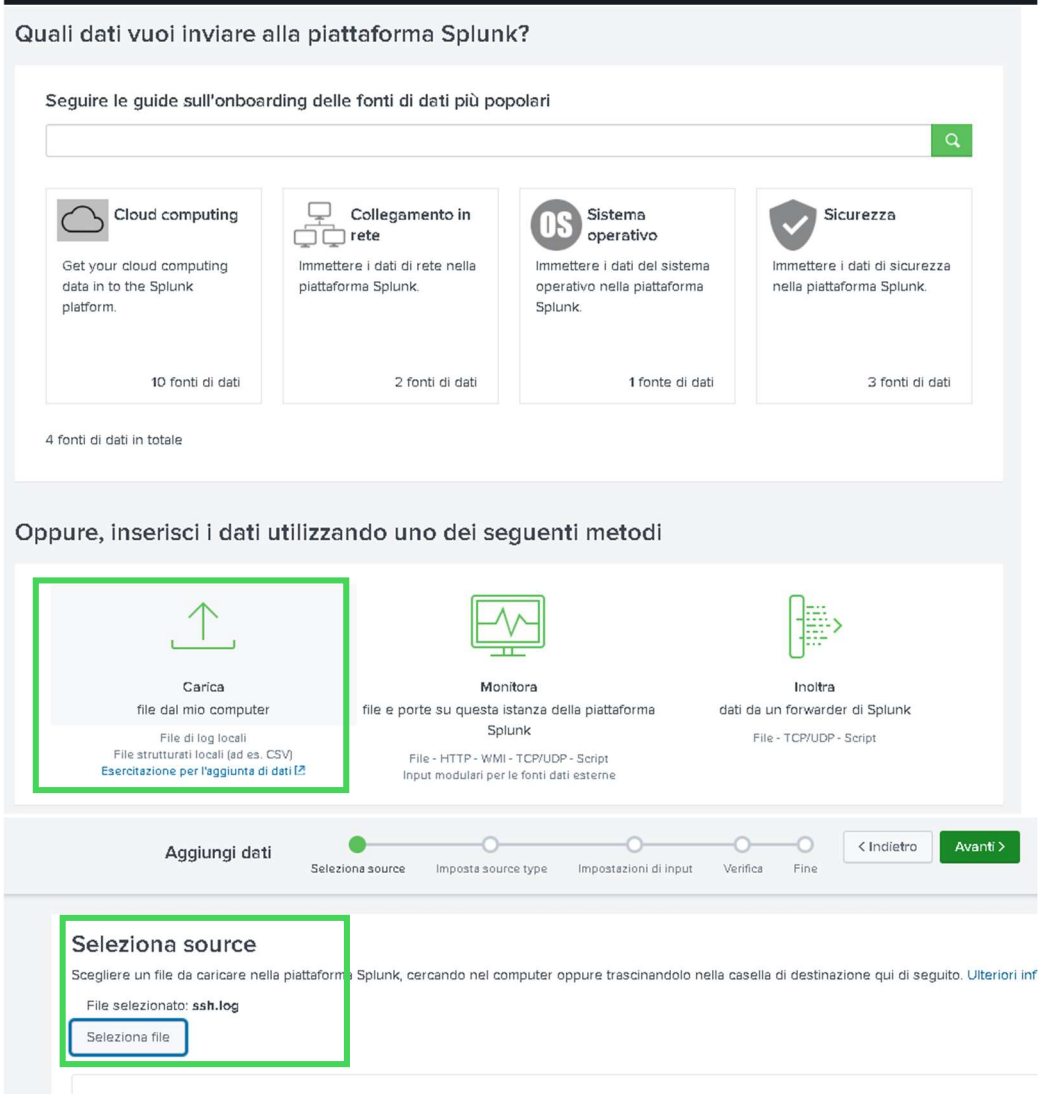
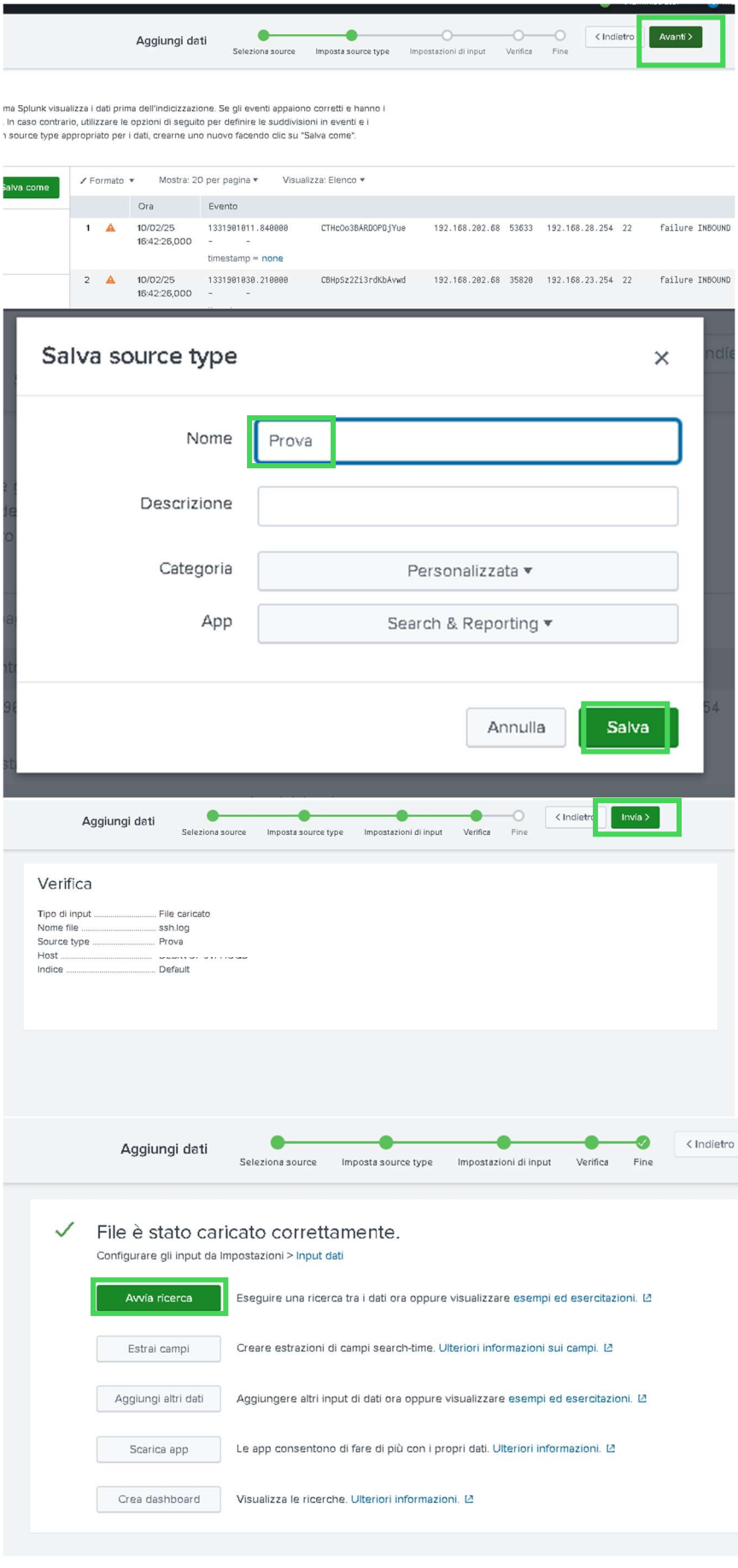
Dopo aver fatto l'accesso a Splunk, sono andato nella sezione Aggiungi dati" e "Carica file dal mio computer" per caricare il file "ssh.log" della consegna:

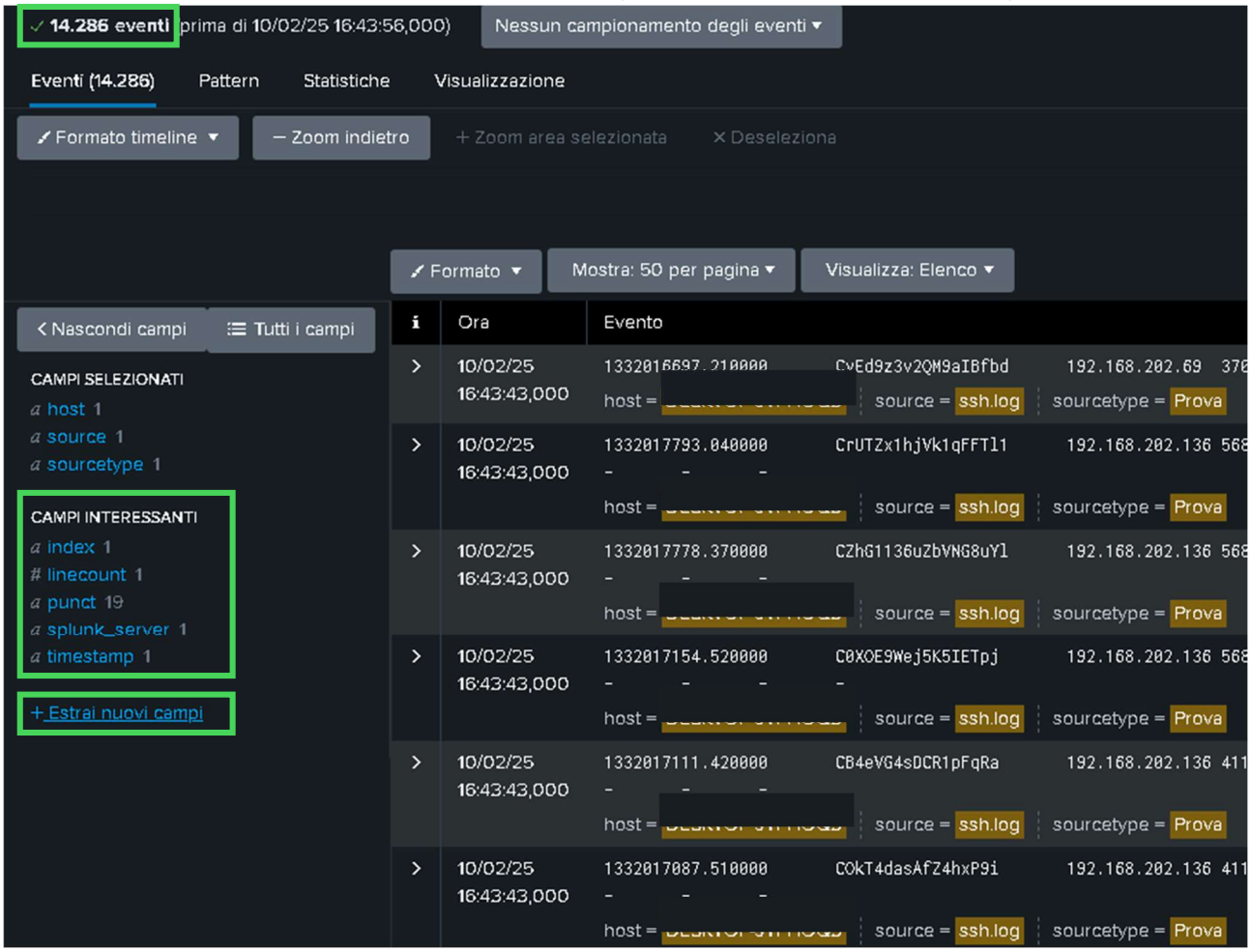




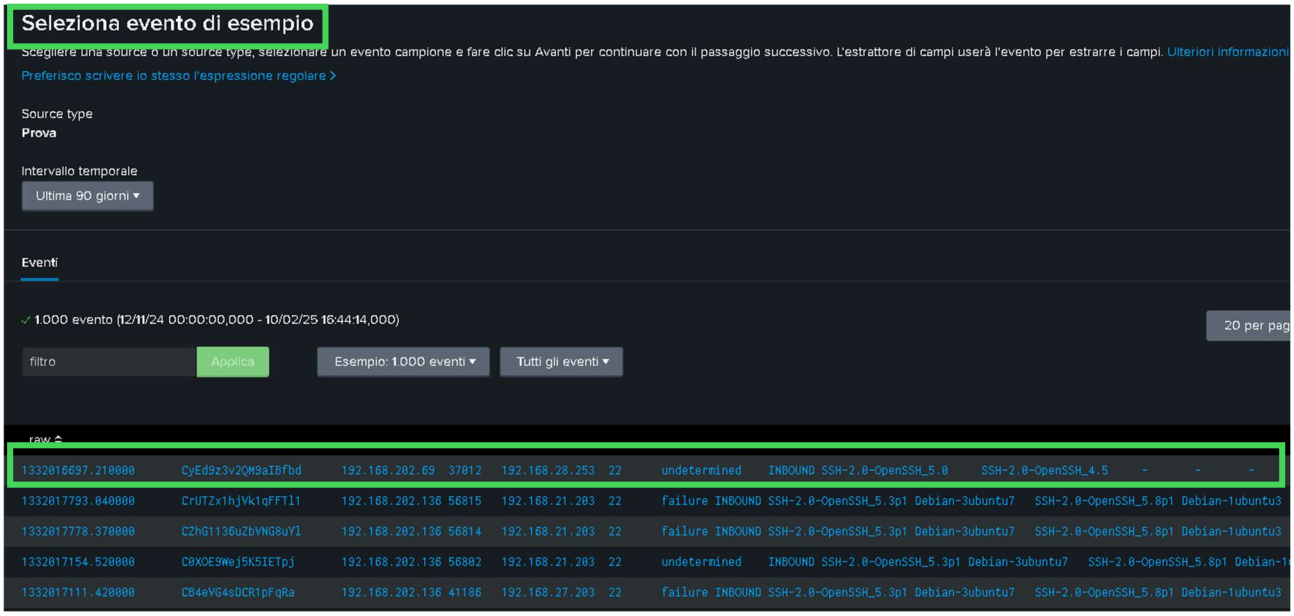
Dopo aver visionato i dati, inserito il source type e lasciando le impostazioni di default, sono arrivato alla schermata dov'era possibile inserire dei filtri per ottimizzare la ricerca:

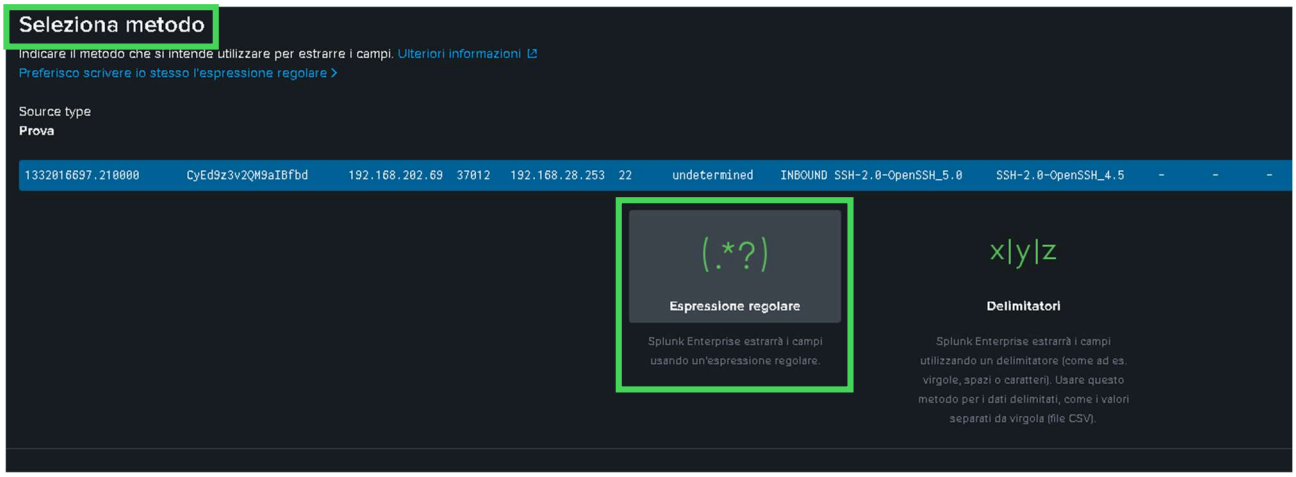


In questa schermata erano presenti tutti gli eventi (14.286) del file di log e andando a vedere nella schermata di sinistra, ho notato che veniva data la possibilità di estrarre nuovi campi dalla ricerca:

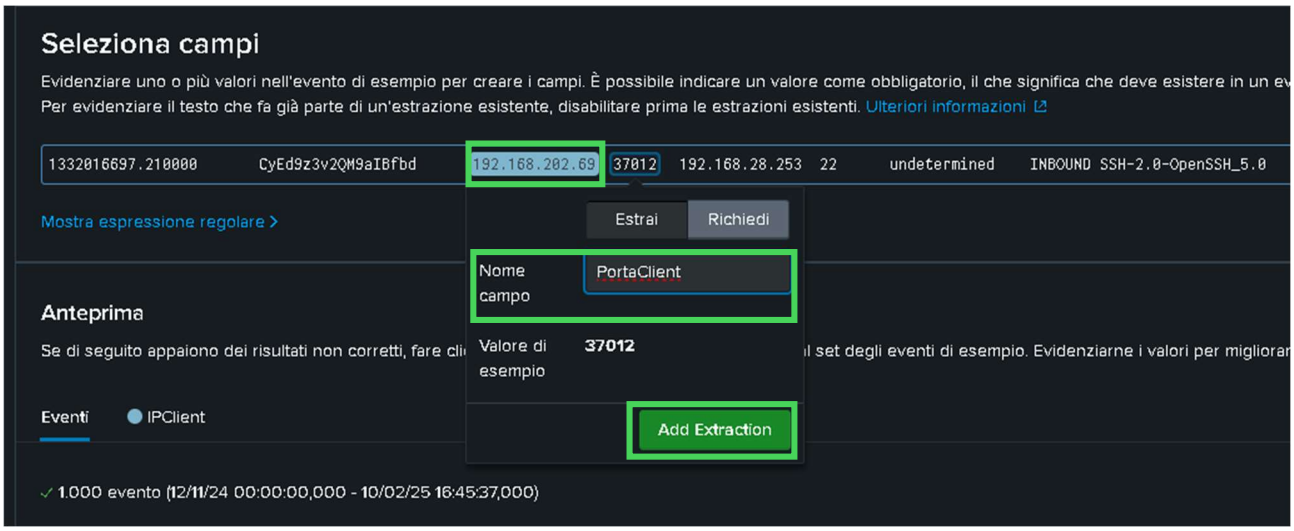


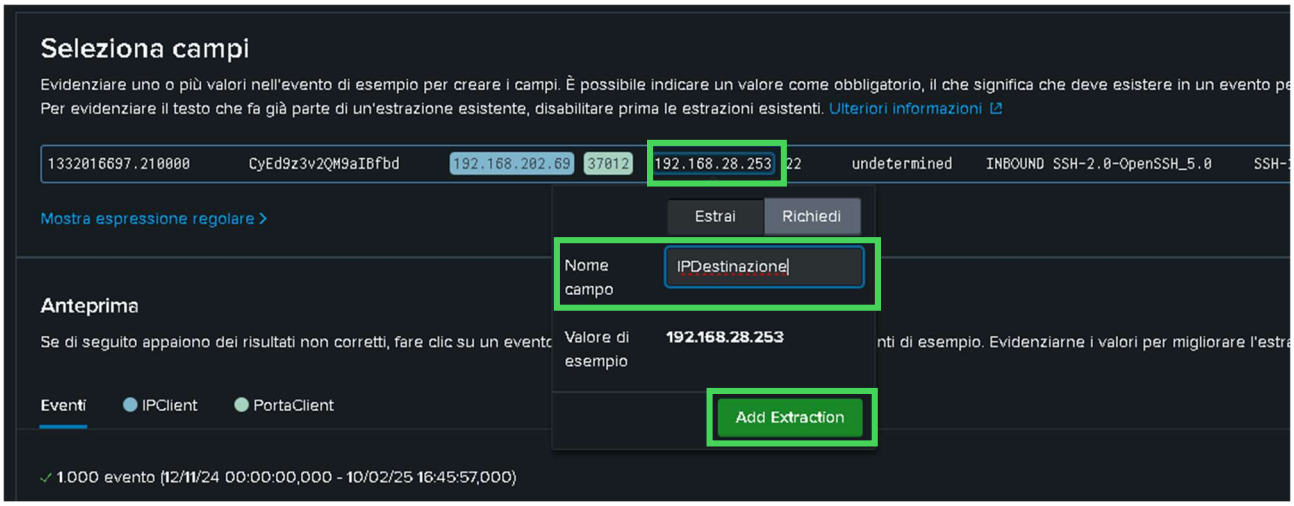
Seleziono il primo evento come evento su cui basare l'inserimento dei campi:





E successivamente selezionato ogni campo che mi interessava, dandogli un nome:

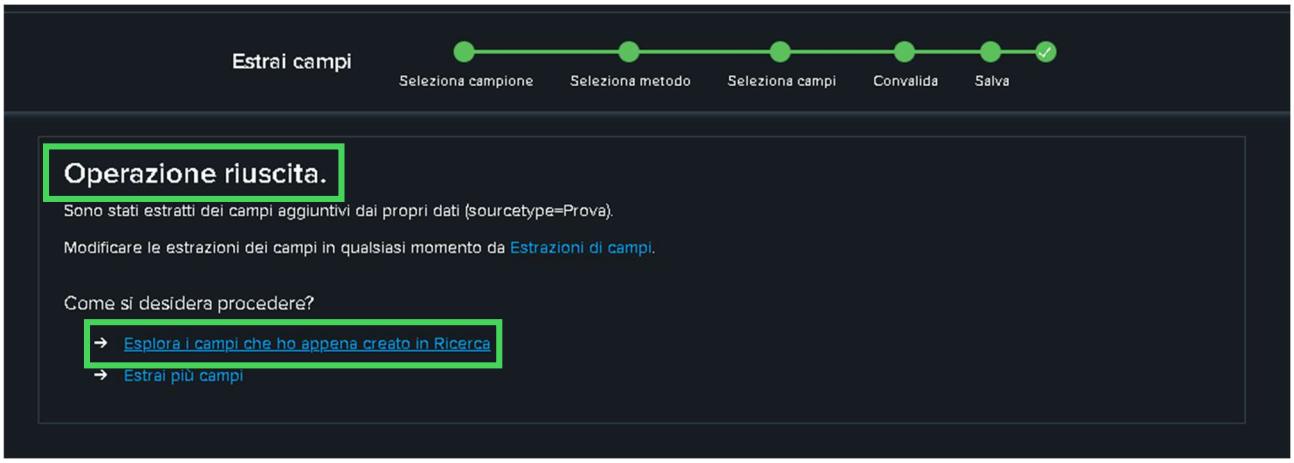



Seleziona campi
Evidenziare uno o più valori nell'evento di esempio per creare i campi. È possibile indicare un valore come obbligatorio, il che significa che deve esistere in un evento pe
Per evidenziare il testo che fa già parte di un'estrazione esistente, disabilitare prima le estrazioni esistenti. Ulteriori informazioni
1332016697.210000 CyEd9z3v2QM9aIBfbd 192.168.202.69 37012 192.168.28.253 22 undetermined INBOUND SSH-2.0-OpenSSH_5.0
Mostra espressione regolare
Estrai Richiedi
Nome campo IPDestinazione
Valore di esempio 192.168.28.253
Anteprima
Se di seguito appaiono dei risultati non corretti, fare clic su un evento
nti di esempio. Evidenziarne i valori per migliorare l'estra
Eventi IPClient PortaClient
Add Extraction
1.000 evento (12/11/24 00:00:00,000 - 10/02/25 16:45:57,000)

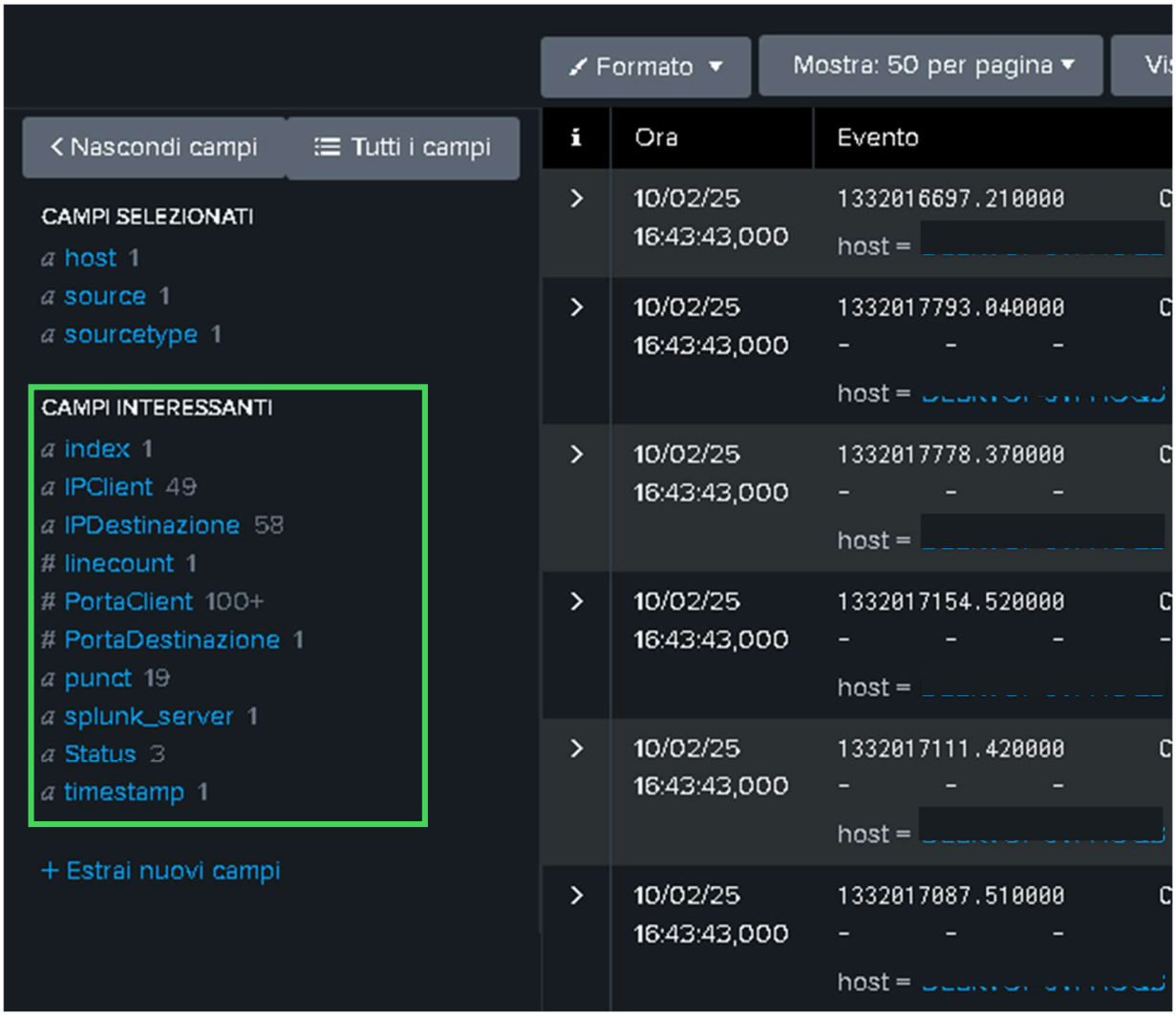

Seleziona campi
Evidenziare uno o più valori nell'evento di esempio per creare i campi. È possibile indicare un valore come obbligatorio, il che significa che deve esistere in un e
Per evidenziare il testo che fa già parte di un'estrazione esistente, disabilitare prima le estrazioni esistenti. Ulteriori informazioni
1332016697.210000 CyEd9z3v2QM9aIBfbd 192.168.202.69 37012 192.168.28.253 22 undetermined INBOUND SSH-2.0-OpenSSH_5.0
Mostra espressione regolare
Estrai Richiedi
Nome campo PortaDestinazione
Valore di esempio 22
Anteprima
Se di seguito appaiono dei risultati non corretti, fare clic su un evento aggiuntivo
pio. Evidenziarne i valori per migliora
Eventi IPClient PortaClient IPDestinazione
Add Extraction
1.000 evento (12/11/24 00:00:00,000 - 10/02/25 16:46:20,000)


Seleziona campi
Evidenziare uno o più valori nell'evento di esempio per creare i campi. È possibile indicare un valore come obbligatorio, il che significa che deve esistere in un ev
Per evidenziare il testo che fa già parte di un'estrazione esistente, disabilitare prima le estrazioni esistenti. Ulteriori informazioni
1332016697.210000 CyEd9z3v2QM9aIBfbd 192.168.202.69 37012 192.168.28.253 22 undetermined INBOUND SSH-2.0-OpenSSH_5.0
Mostra espressione regolare
Estrai Richiedi
Nome campo Status
Valore di esempio undetermined
Anteprima
Se di seguito appaiono dei risultati non corretti, fare clic su un evento aggiuntivo per aggiunger
he i valori per migliorar
Eventi IPClient PortaClient IPDestinazione PortaDestinazione
Add Extraction
1.000 evento (12/11/24 00:00:00,000 - 10/02/25 16:46:42,000)

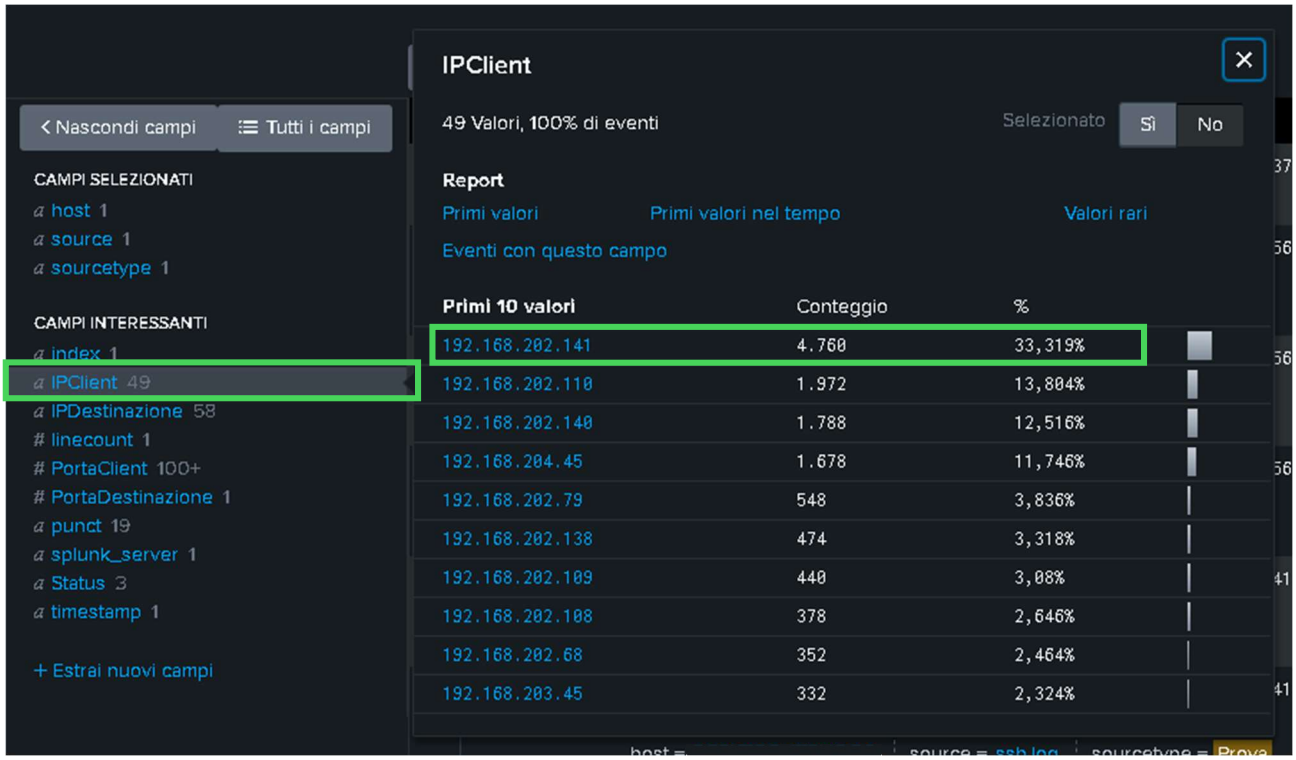
Dopo aver completato l'inserimento dei campi, ho visualizzato la nuova schermata di ricerca:



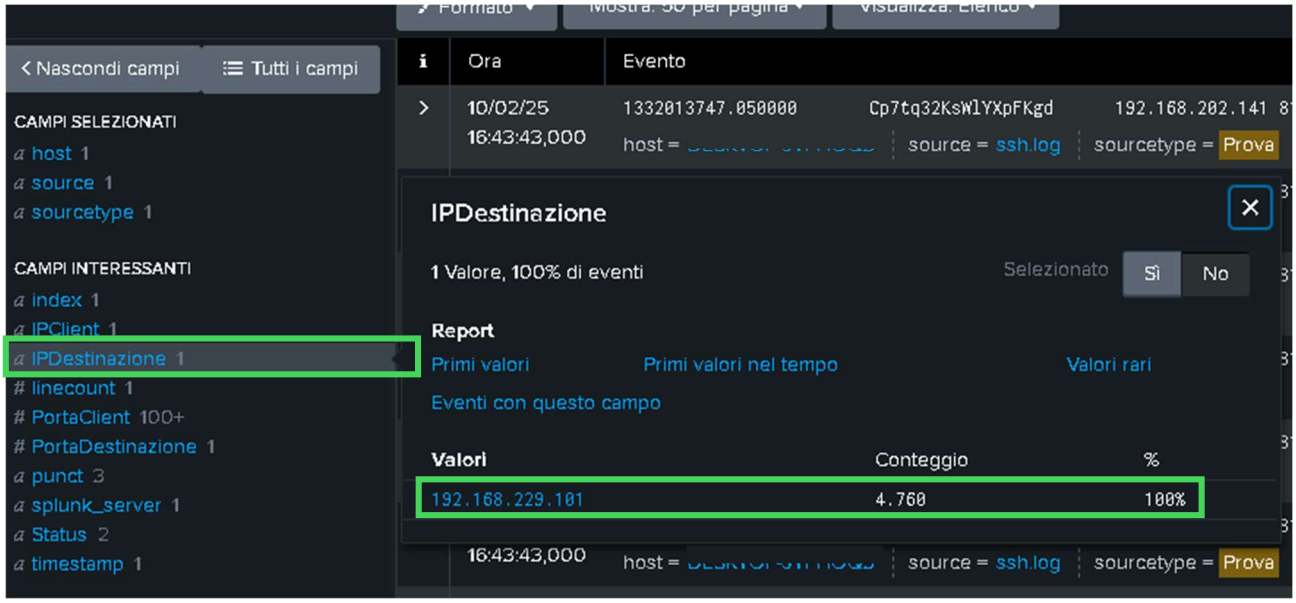
Nottando che erano presenti altri campi più ordinati e interessanti



Andando a selezionare “IPClient” era comparsa una schermata che indicava la percentuale di eventi legata a quel campo.
Nella schermata quindi era presente che l’IP 192.168.202.141 era presente negli eventi il 33% per 4.760 volte e andando a ciccarlo, si aggiungeva nella query di ricerca, riducendo al minimo la ricerca



Ho visualizzato poi l’IP destinazione notando che l’IP 192.168.229.101 era presente al 100% in tutti gli eventi riguardanti il precedente indirizzo IP client



Dato che gli eventi erano tutti sulla porta 22, ho supposto che si trattasse di un attacco brute force dalla macchina 192.168.202.141 verso la macchina 192.168.229.101 usando il servizio SSH.