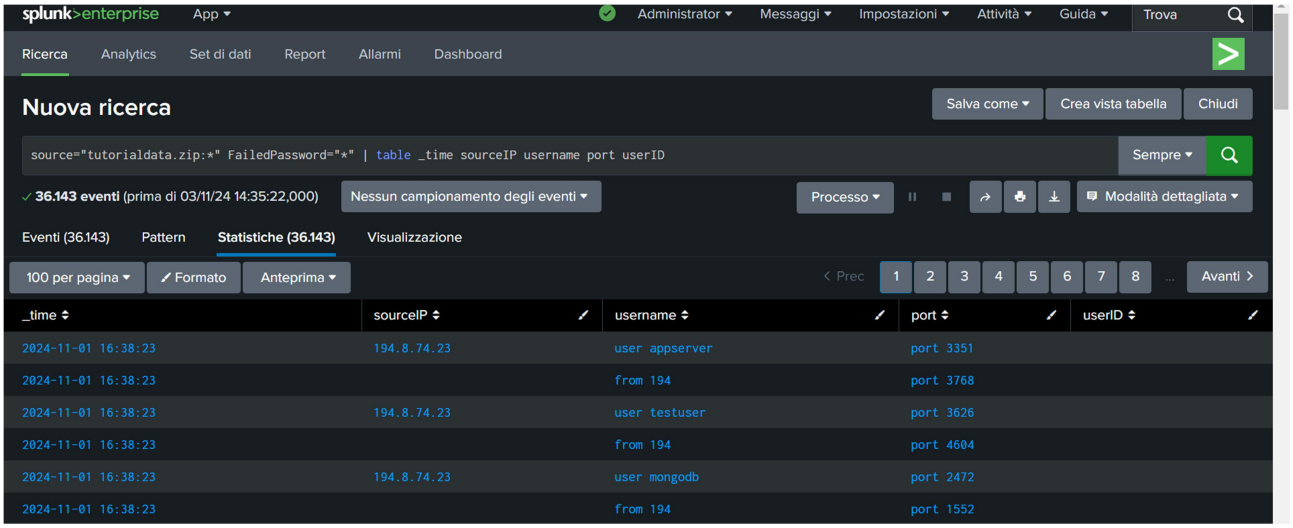
Benchmark M6 – Daniele Rufo

Come richiesto dall'esercizio ecco le query.

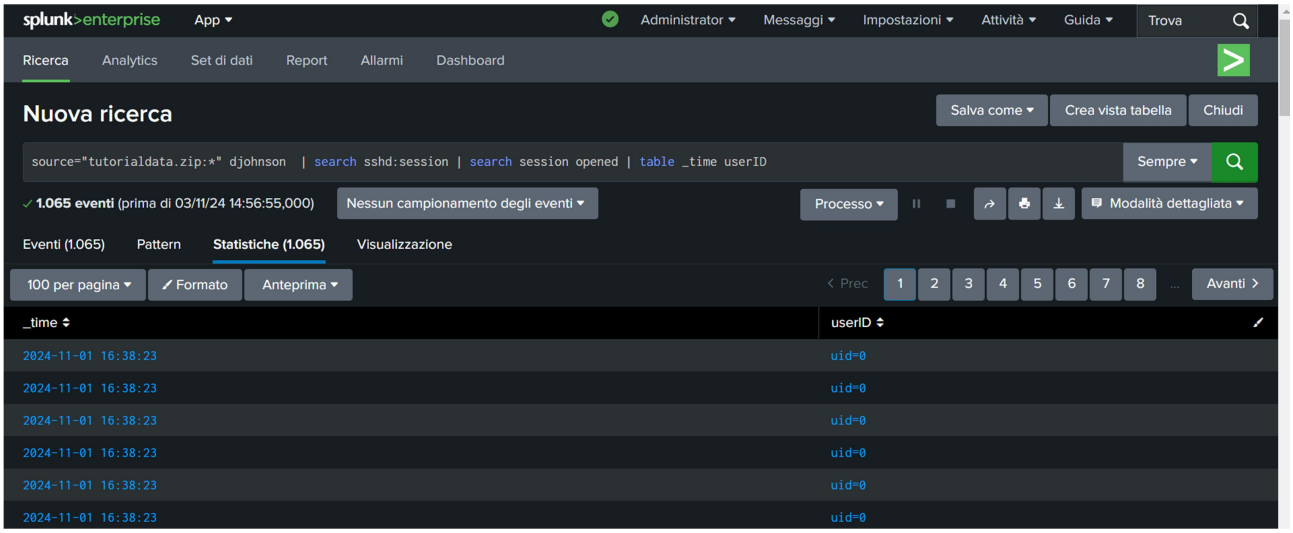
Per lo svolgimento è stato necessario creare nuovi campi per modificare il parsing ed allinearlo alle esigenze di ogni richiesta. Purtroppo il parsing dei nuovi campi (username – sourceIP – port) non risulta perfetto anzi tralascia qualche risultato, lo legge nel modo sbagliato ecc. Li ho creati usando l'interfaccia grafica di Splunk poichè non sapevo usare le "regular expressions" manualmente, nonostante ciò deve esserci qualcosa che mi sfugge perché il risultato è imperfetto. Con i miei strumenti sono riuscito ad arrivare fino a qui, avrei bisogno di più tempo e di uno studio vero del software (quindi tempo) per poter andare oltre.

Negli screenshot si può vedere la query nella barra di ricerca:

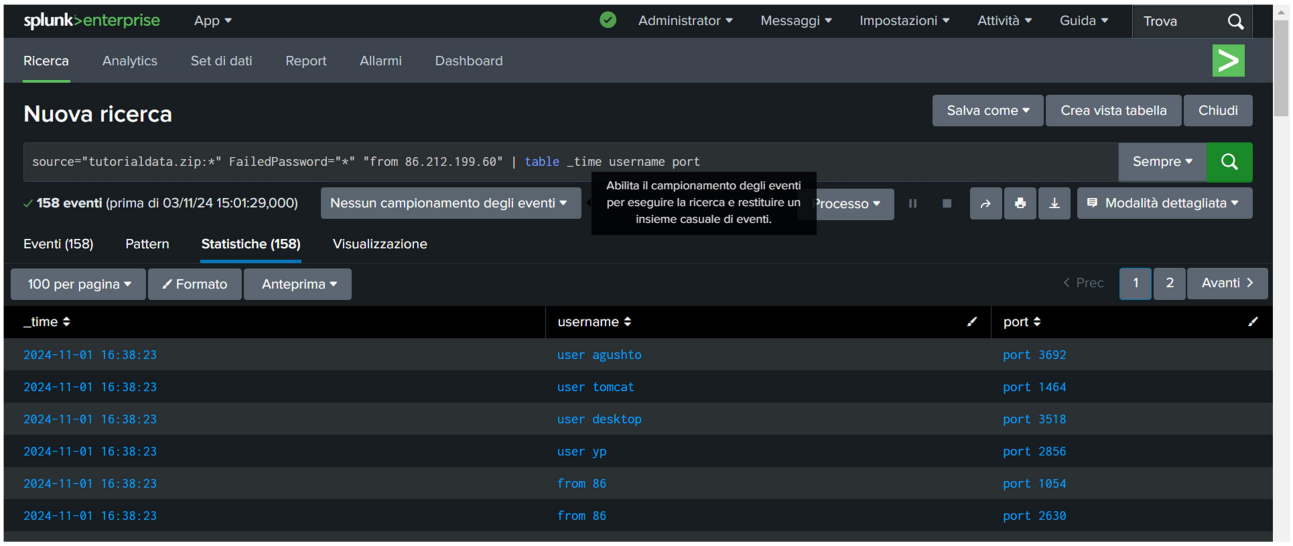
1



2

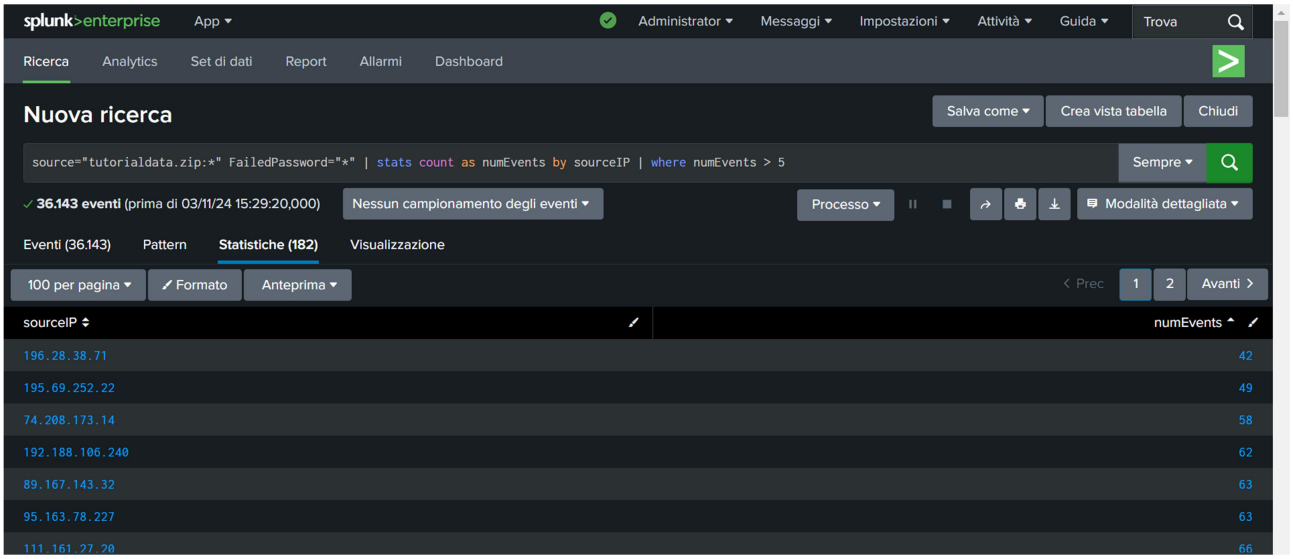


3



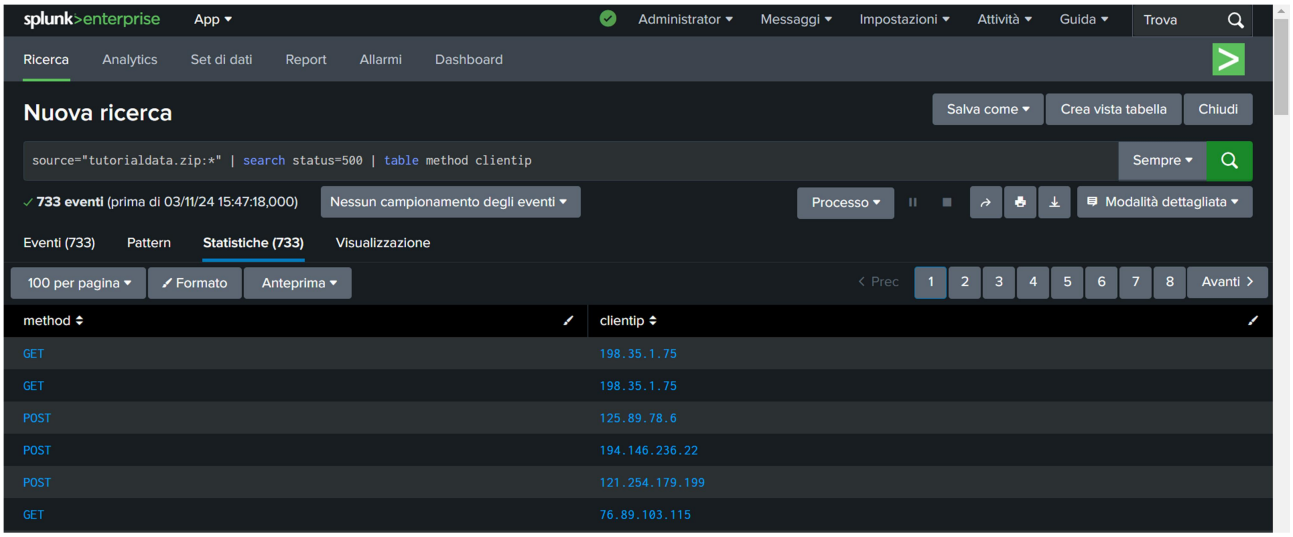
Inizialmente questa query prevedeva la selezione del campo “sourceIP” con cui selezionavo i risultati per l’IP di nostro interesse. Tuttavia, per il problema di creazione campi menzionato sopra, mi sono accorto che il parsing era incompleto quindi, osservando prima l’errore, ho sostituito il campo con un filtro inserito come stringa “from 86.212.199.60” ed infatti gli eventi trovati salgono da 112 a 158.

4



Ho provato diverse metodologie cercando una soluzione il più semplice possibile e adeguata alle mie conoscenze. Mi sono aiutato rinominando “numEvents” il numero di tentativi indicizzandoli per indirizzo IP e poi ho preso questo output e l’ho sottoposto alla condizione “numEvents>5” per il ritorno esclusivo dei dati richiesti.

5



Ho aggiunto una visualizzazione tabellare che riporta metodo della richiesta http e client IP per avere una visione più completa poiché credo siano info utili per “Internal Server Error”

Grazie

Daniele Rufo