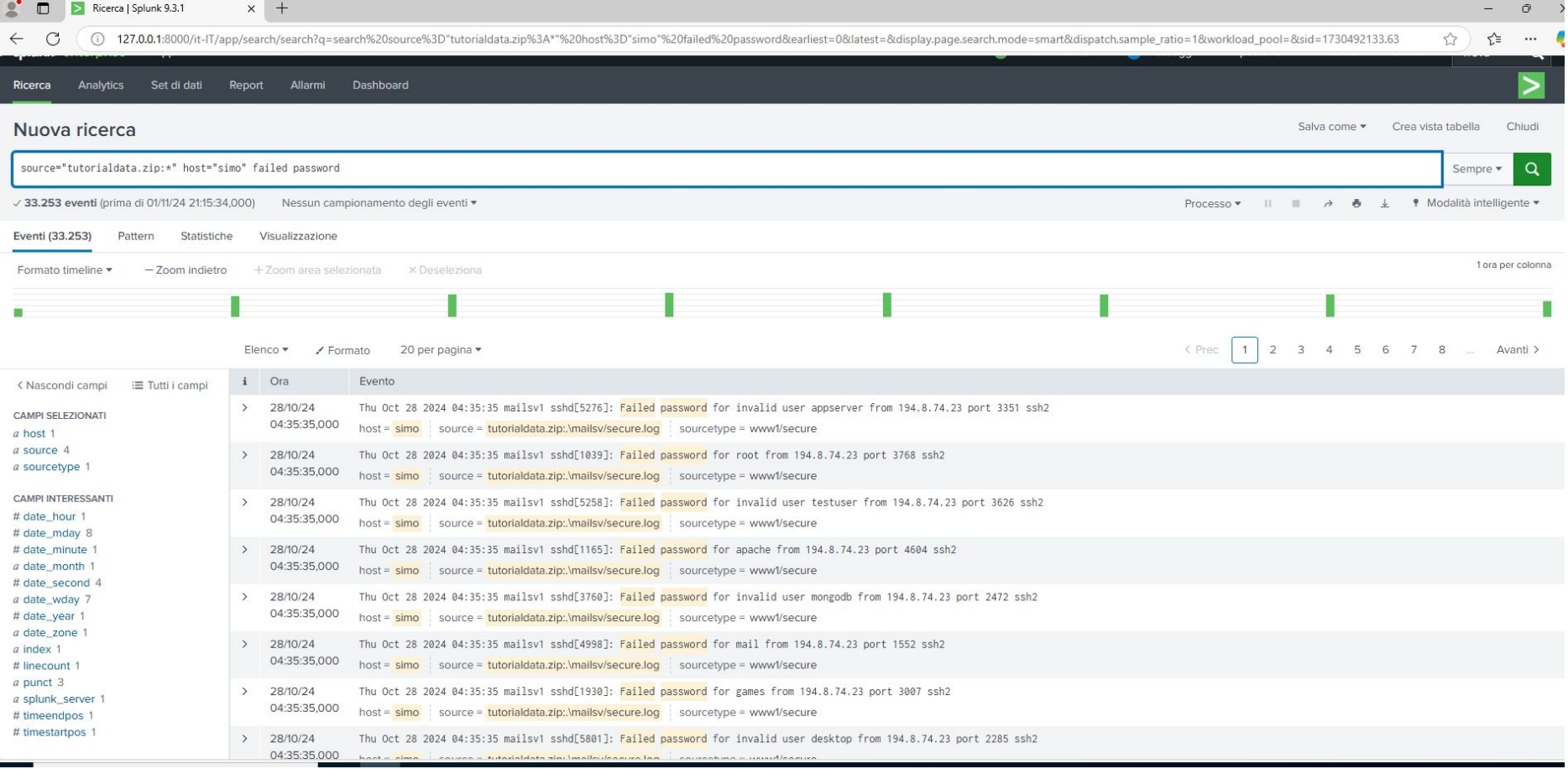
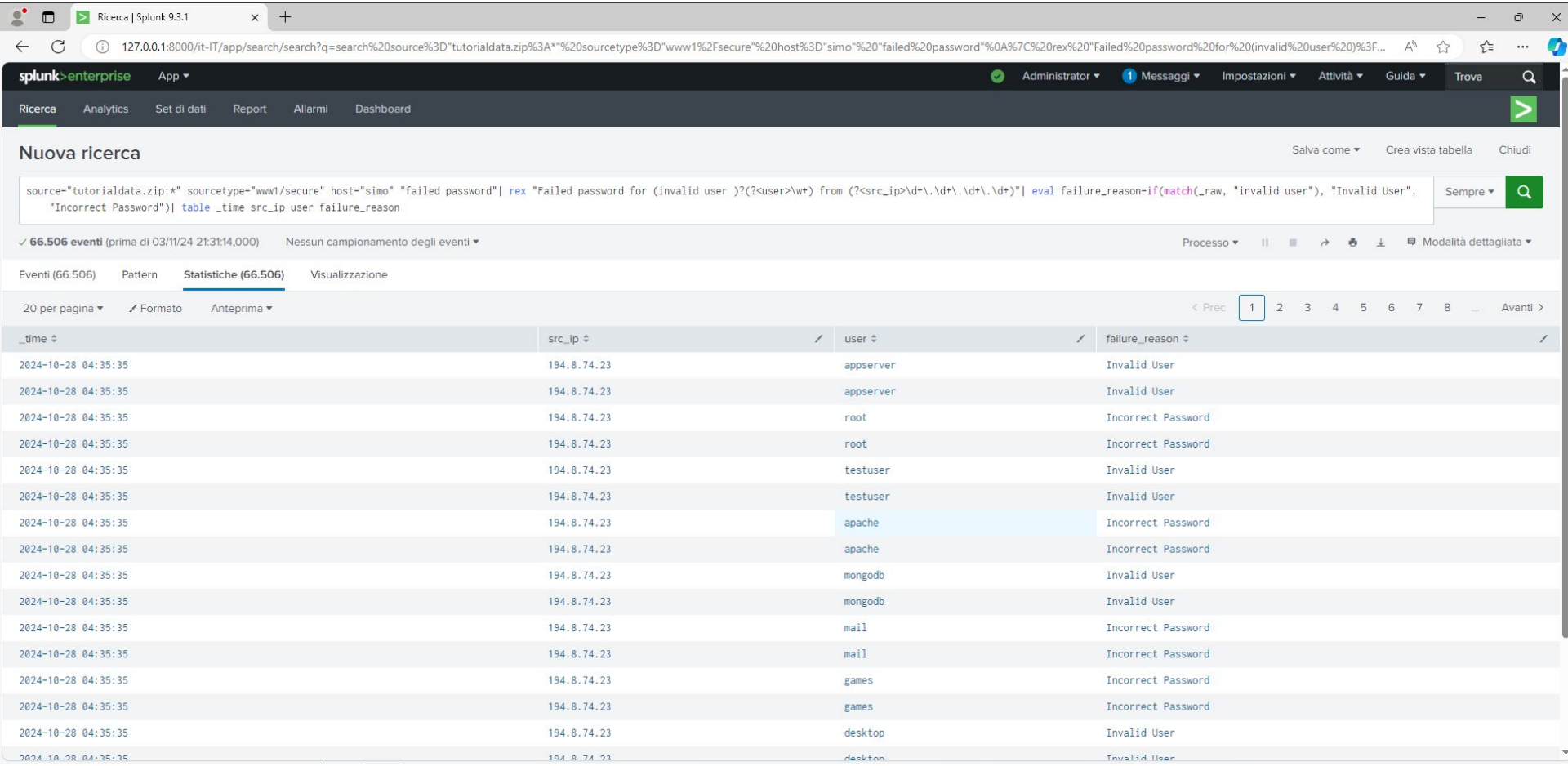
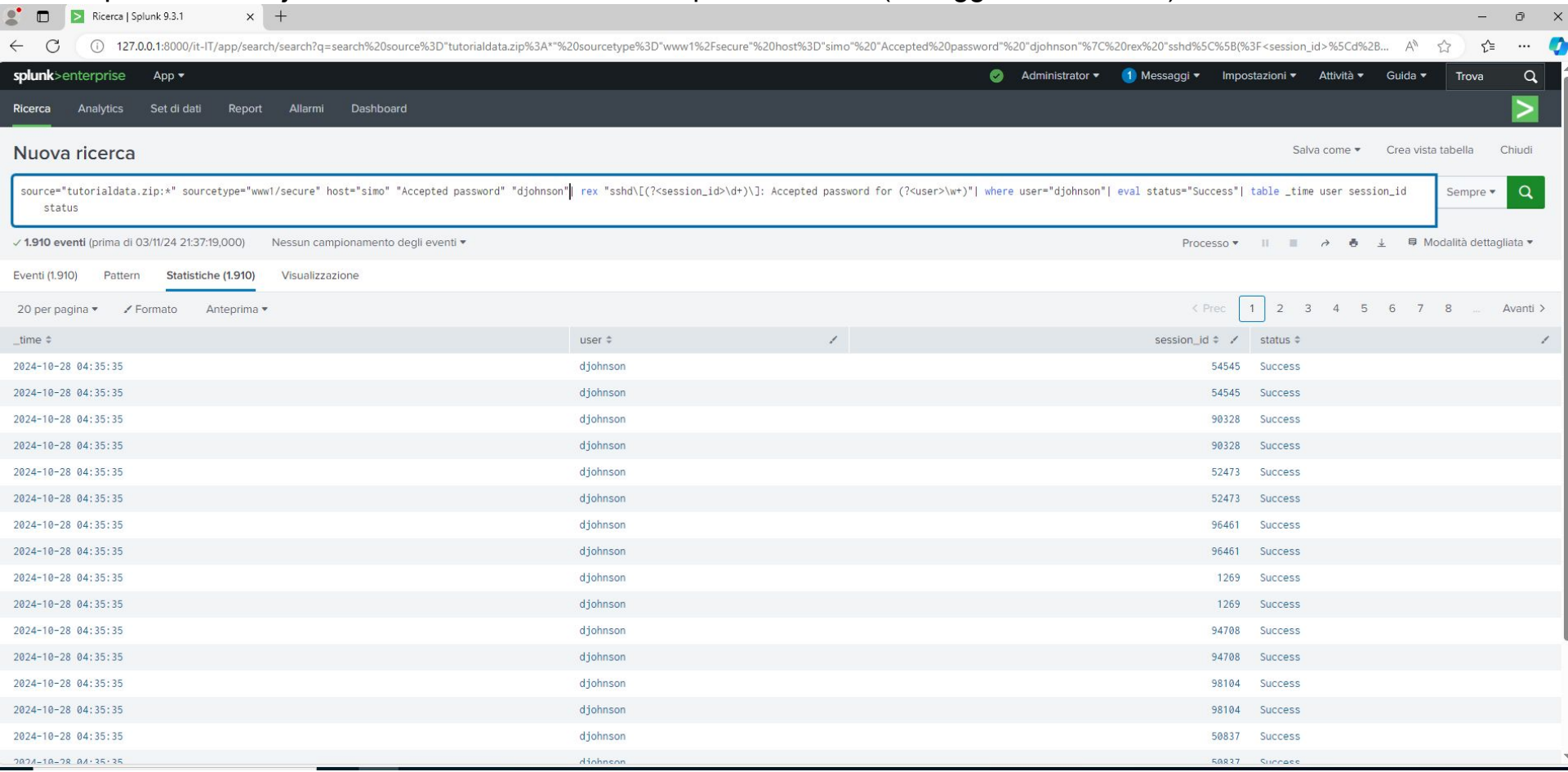

Ricerca | Splunk 9.3.1
127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"tutorialdata.zip%3A*"%20host%3D"simo"%20failed%20password&earliest=0&latest=&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&sid=1730492133.63
Ricerca
Analytics
Set di dati
Report
Allarmi
Dashboard
Nuova ricerca
Salva come
Crea vista tabella
Chiudi
source="tutorialdata.zip:*" host="simo" failed password
Sempre
33.253 eventi (prima di 01/11/24 21:15:34,000)
Nessun campionamento degli eventi
Processo
Modalità intelligente
Eventi (33.253)
Pattern
Statistiche
Visualizzazione
Formato timeline
Zoom indietro
Zoom area selezionata
Deseleziona
1 ora per colonna
Elenco
Formato
20 per pagina
Prec
1
2
3
4
5
6
7
8
Avanti
Nascondi campi
Tutti i campi
CAMPI SELEZIONATI
a host 1
a source 4
a sourcetype 1
CAMPI INTERESSANTI
date_hour 1
date_mday 8
date_minute 1
a date_month 1
date_second 4
a date_wday 7
date_year 1
a date_zone 1
a index 1
linecount 1
a punct 3
a splunk_server 1
timeendpos 1
timestartpos 1
Ora
Evento
28/10/24 04:35:35,000
Thu Oct 28 2024 04:35:35 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2
host = simo source = tutorialdata.zip:.\mailsv/secure.log sourcetype = www1/secure
28/10/24 04:35:35,000
Thu Oct 28 2024 04:35:35 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2
host = simo source = tutorialdata.zip:.\mailsv/secure.log sourcetype = www1/secure
28/10/24 04:35:35,000
Thu Oct 28 2024 04:35:35 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2
host = simo source = tutorialdata.zip:.\mailsv/secure.log sourcetype = www1/secure
28/10/24 04:35:35,000
Thu Oct 28 2024 04:35:35 mailsv1 sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2
host = simo source = tutorialdata.zip:.\mailsv/secure.log sourcetype = www1/secure
28/10/24 04:35:35,000
Thu Oct 28 2024 04:35:35 mailsv1 sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2
host = simo source = tutorialdata.zip:.\mailsv/secure.log sourcetype = www1/secure
28/10/24 04:35:35,000
Thu Oct 28 2024 04:35:35 mailsv1 sshd[4998]: Failed password for mail from 194.8.74.23 port 1552 ssh2
host = simo source = tutorialdata.zip:.\mailsv/secure.log sourcetype = www1/secure
28/10/24 04:35:35,000
Thu Oct 28 2024 04:35:35 mailsv1 sshd[1930]: Failed password for games from 194.8.74.23 port 3007 ssh2
host = simo source = tutorialdata.zip:.\mailsv/secure.log sourcetype = www1/secure
28/10/24 04:35:35,000
Thu Oct 28 2024 04:35:35 mailsv1 sshd[5801]: Failed password for invalid user desktop from 194.8.74.23 port 2285 ssh2

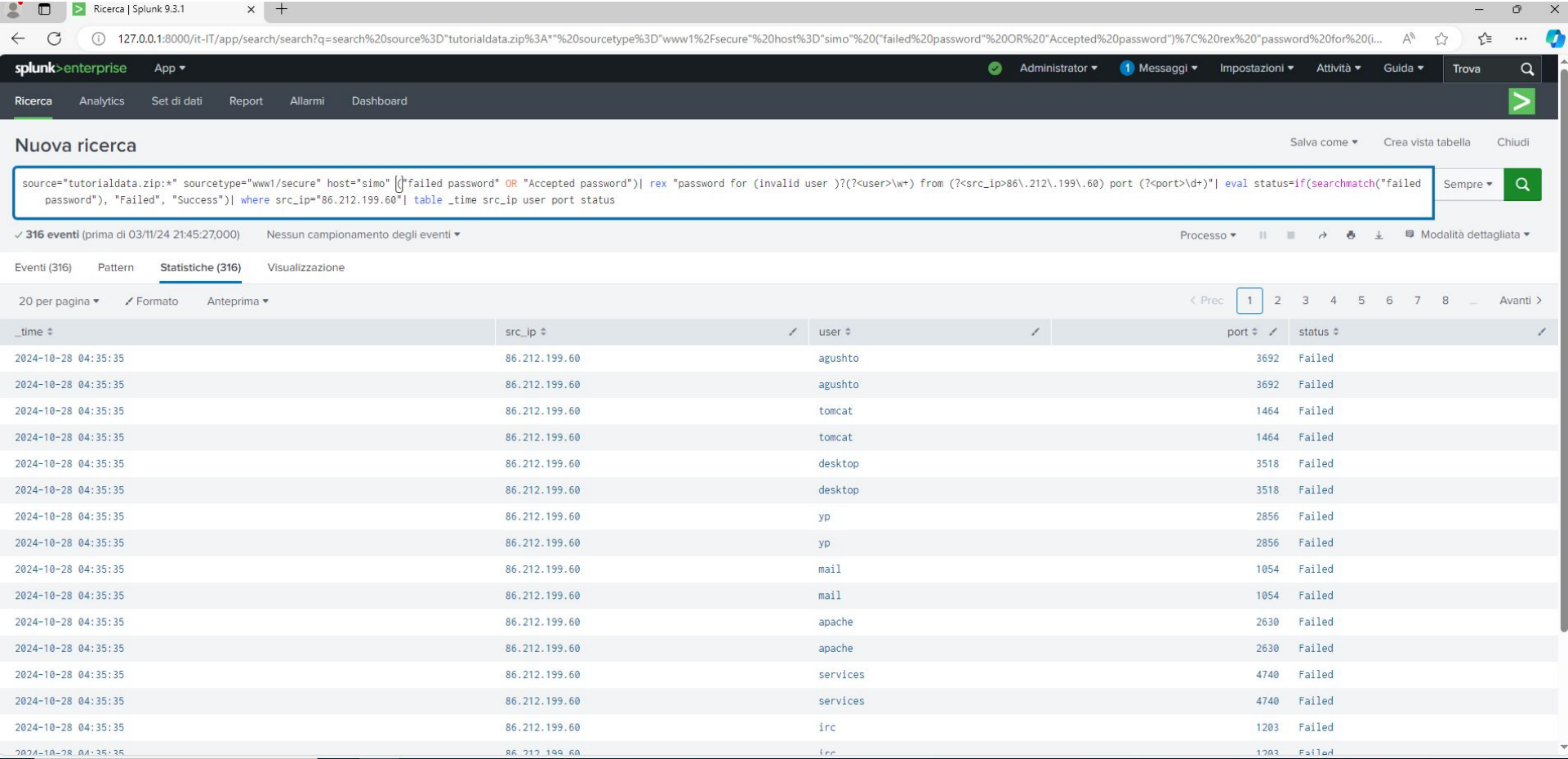
1a query:Crea una query Splunk per identificare tutti i tentativi di accesso falliti "Failed password". La query dovrebbe mostrare il timestamp, l'indirizzo IP di origine, il nome utente e il motivo del fallimento.



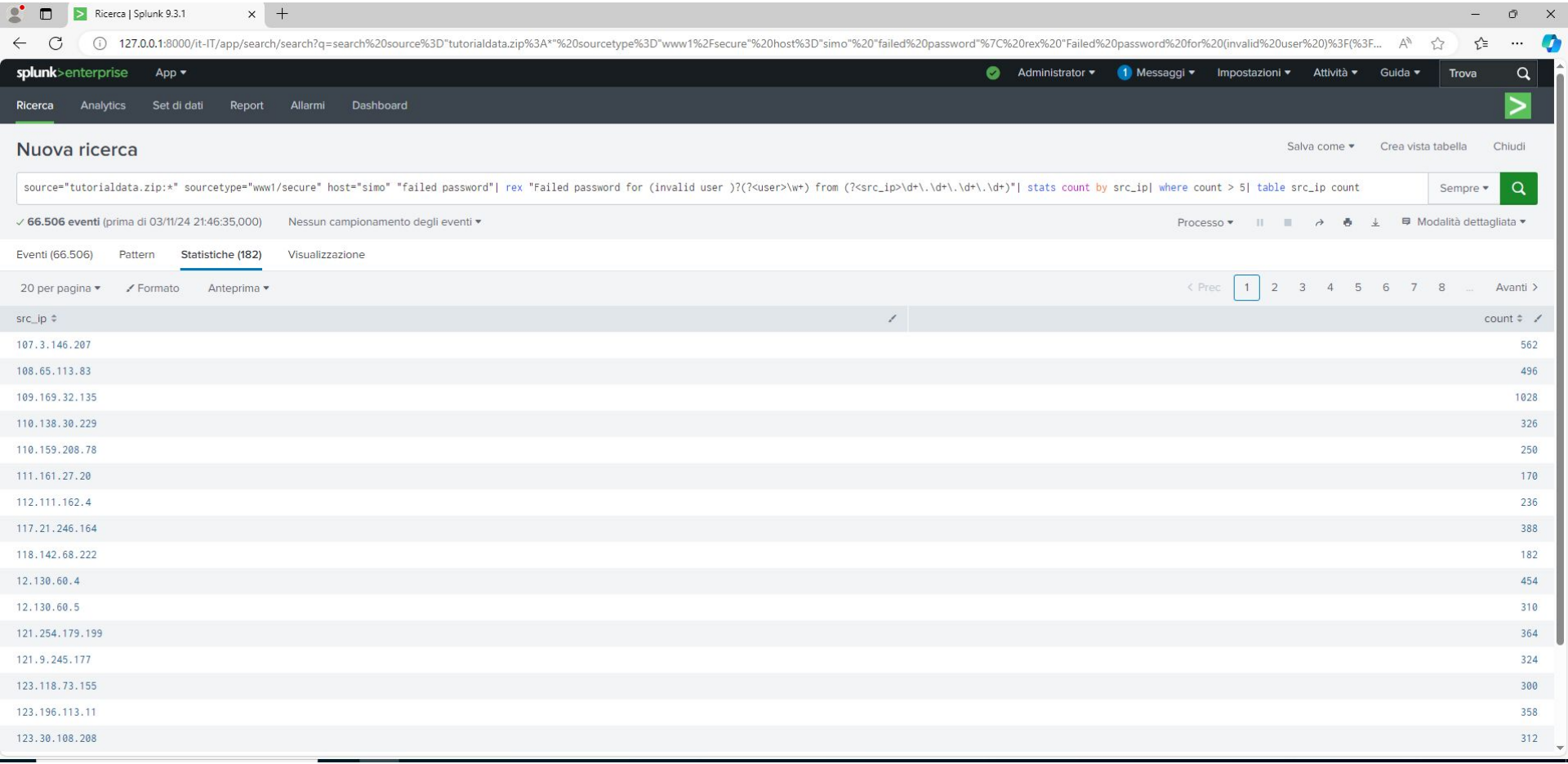
2a query:Scrivi una query Splunk per trovare tutte le sessioni SSH aperte con successo. La query dovrebbe filtrare per l'utente “djohnson” e mostrare il timestamp e l'ID utente.(Ho aggiunto lo status)



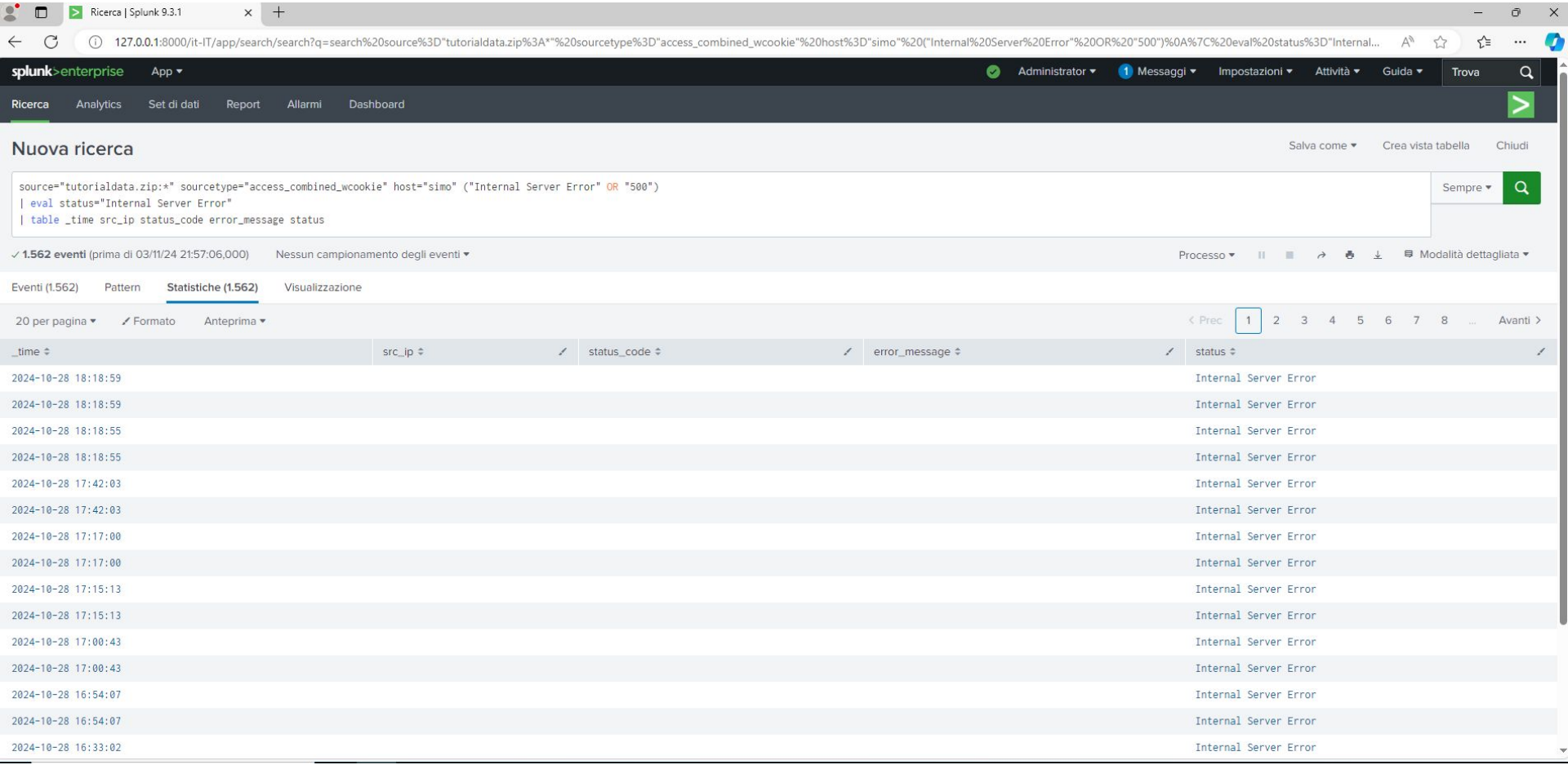
3a query:Scrivi una query Splunk per trovare tutti i tentativi di accesso falliti provenienti dall'indirizzo IP “86.212.199.60”. La query dovrebbe mostrare il timestamp, il nome utente e il numero di porta.(Ho aggiunto lo status)



4a query:Crea una query Splunk per identificare gli indirizzi IP che hanno tentato di accedere ("Failed password") al sistema più di 5 volte. La query dovrebbe mostrare l'indirizzo IP e il numero di tentativi.



5a query:Crea una query Splunk per trovare tutti gli Internal Server Error



Dalle analisi eseguite con le query Splunk, è possibile trarre alcune conclusioni sui log analizzati. Utilizzando tecniche di intelligenza artificiale per identificare pattern e anomalie, possiamo ottenere una visione più approfondita degli eventi e delle potenziali vulnerabilità nella sicurezza del sistema.

Conclusioni Basate sui Log Analizzati

1. **Tentativi di Accesso Falliti**:
   - Dai tentativi di accesso falliti ("Failed password"), emerge che ci sono indirizzi IP che tentano ripetutamente di accedere al sistema senza successo. Questo potrebbe indicare:
     - **Attività di forza bruta**: IP che effettuano numerosi tentativi di accesso falliti possono rappresentare un tentativo di forza bruta, dove un attaccante cerca di indovinare le credenziali.
     - **Possibile abuso di credenziali**: Alcuni nomi utente specifici possono essere ripetutamente presi di mira, suggerendo che l'attaccante potrebbe avere alcune informazioni preliminari sulle credenziali valide.
2. **Accessi SSH di Successo per Utente Specifico**:
   - Le sessioni SSH aperte con successo dall'utente "djohnson" mostrano che questo utente ha effettuato accessi regolari e legittimi. Tuttavia:
     - **Monitoraggio eccessivo per utenti privilegiati**: L'utente `djohnson` potrebbe essere un account amministrativo. È importante monitorare gli accessi SSH per garantire che non ci siano attività anomale legate a questo account, come accessi fuori orario o da IP insoliti.
3. **Tentativi di Accesso da un IP Specifico**:
   - Analizzando i tentativi di accesso falliti provenienti dall'indirizzo IP `86.212.199.60`, si nota che questo IP ha tentato di accedere ripetutamente al sistema. Questo tipo di attività può suggerire:
     - **Attività sospette o dannose**: Questo IP potrebbe far parte di un attacco mirato al sistema, con tentativi di accesso ripetuti verso utenti specifici e su porte specifiche, il che può aiutare a identificare i tentativi di exploit mirati.
     - **IP nella blacklist**: Considerare l'aggiunta di questo IP alla blacklist o a un sistema di rilevamento delle intrusioni (IDS) per bloccare i tentativi futuri.
4. **Indirizzi IP con Più di 5 Tentativi di Accesso Falliti**:
   - Gli indirizzi IP con più di 5 tentativi di accesso falliti rappresentano una minaccia potenziale. I pattern identificati qui indicano:
     - **Potenziale attacco di forza bruta distribuita**: Se ci sono molti IP che effettuano tentativi ripetuti, potrebbe trattarsi di un attacco coordinato dove più IP tentano di forzare l'accesso al sistema.
     - **Segmentazione degli attacchi**: In alcuni casi, attacchi di questo tipo possono essere distribuiti nel tempo per evitare di essere rilevati dai sistemi di sicurezza. È importante monitorare continuamente tali IP e implementarli in un firewall o sistema di prevenzione delle intrusioni.
5. **Errori di Server Interno (Internal Server Error)**:
   - Gli errori "Internal Server Error" (500) possono essere un indicatore di problemi nei servizi interni o nelle applicazioni web. Se questi errori sono frequenti, suggeriscono:
     - **Problemi di configurazione o codice**: Gli errori 500 possono derivare da errori di configurazione o da problemi nel codice dell'applicazione. È importante che il team di sviluppo riveda i log degli errori per identificare la causa principale.
     - **Possibile vettore di attacco**: Gli errori 500, soprattutto se associati a input dell'utente, possono rivelare vulnerabilità che un attaccante potrebbe sfruttare per eseguire attacchi di iniezione o altre tecniche di exploit.

Raccomandazioni

- **Implementare sistemi di rilevamento delle intrusioni (IDS)**: Per monitorare e bloccare gli IP sospetti che tentano accessi ripetuti.
- **Analisi dei Log Periodica**: Automatizzare l'analisi dei log per rilevare in modo proattivo attività sospette come tentativi di forza bruta.
- **Miglioramento del monitoraggio dell'applicazione**: Ridurre la frequenza degli errori 500, per prevenire esposizioni accidentali di informazioni sensibili.
- **Utilizzo di meccanismi di rate limiting e blocco IP**: Limitare il numero di tentativi di accesso consentiti in un breve periodo di tempo per mitigare attacchi di forza bruta.

Queste misure, insieme a un monitoraggio continuo e l'uso di algoritmi di rilevamento delle anomalie basati su AI, possono migliorare significativamente la sicurezza del sistema e prevenire accessi non autorizzati e interruzioni del servizio.