PROGETTO FINALE W24D4

TRACCIA:

Importare su Splunk i dati di *tutorialdata.zip*

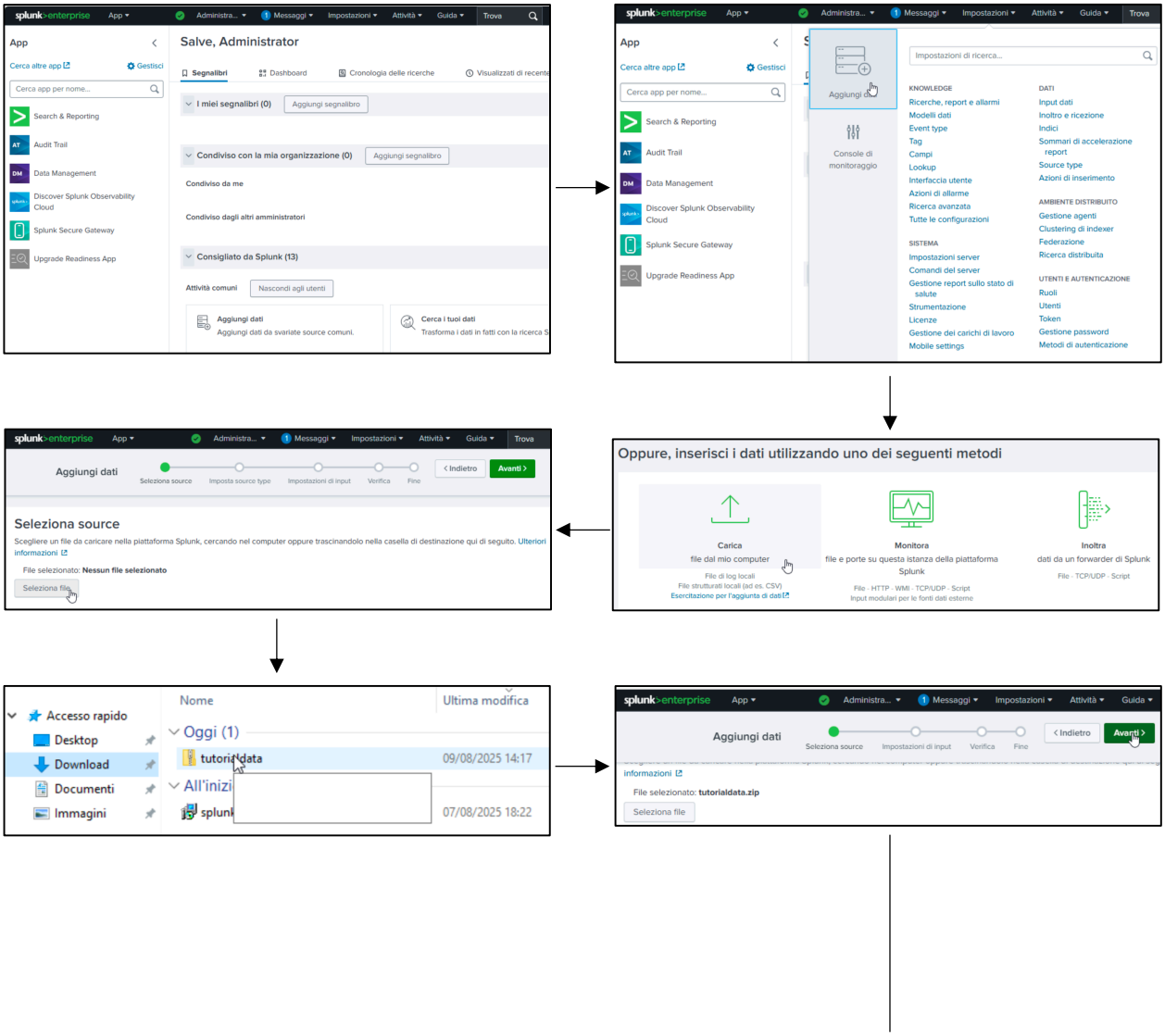
1. Creare una query per identificare tutti i tentativi di accesso falliti "Failed Password".
   La query dovrebbe mostrare timestamp, indirizzo IP di origine, nome utente e motivo del fallimento.
2. Scrivere una query per trovare tutte le sessioni SSH aperte con successo.
   La query dovrebbe filtrare per l'utente "djohnson" e mostrare timestamp e ID utente.
3. Scrivere una query per trovare tutti i tentativi di accesso falliti provenienti dall'IP 86.212.199.60.
   La query dovrebbe mostrare timestamp, nome utente e numero porta.
4. Creare una query per identificare gli indirizzi IP che hanno tentato di accedere al sistema più di 5 volte.
   La query dovrebbe mostrare IP e numero di tentativi.
5. Creare una query per trovare tutti gli Internal Server Error.

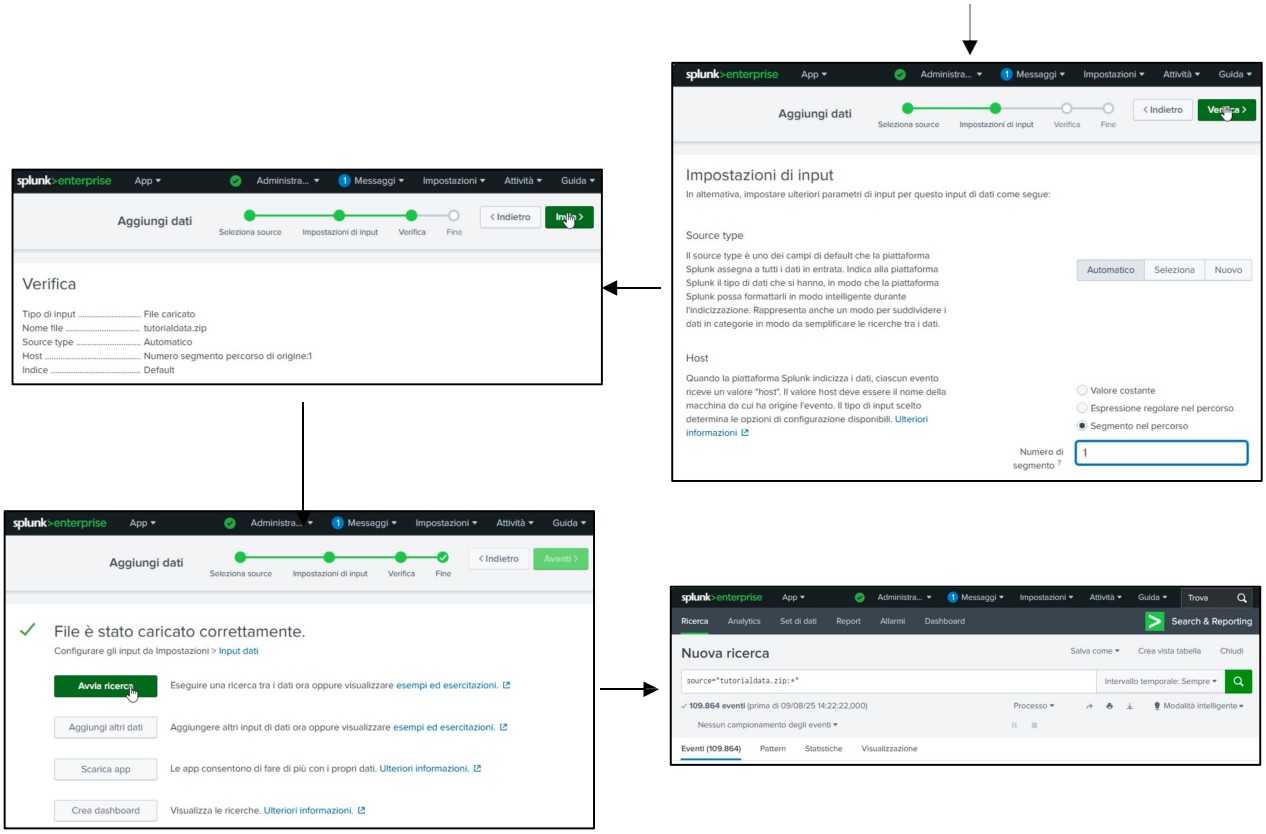
Infine trarre delle conclusioni sui log analizzati utilizzando AI.

SOLUZIONE:

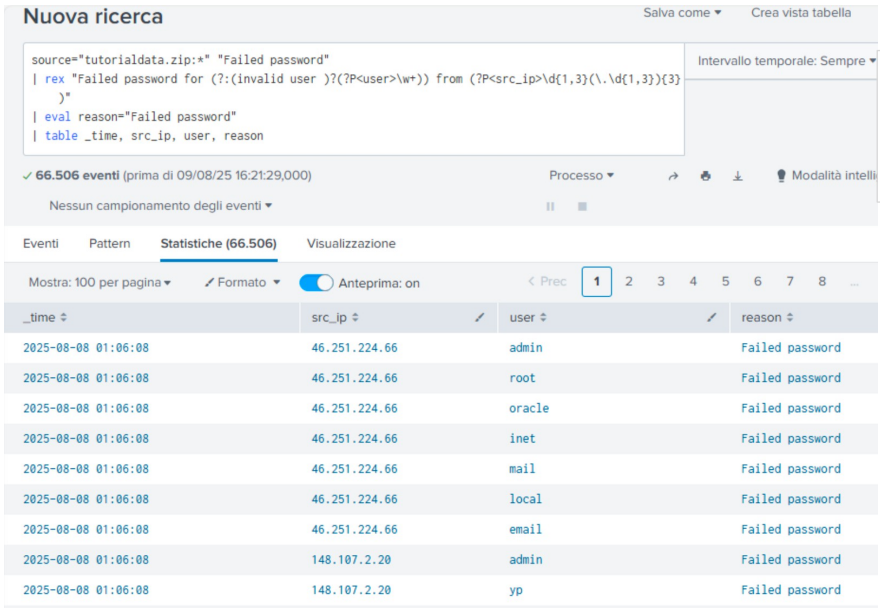
Importare *tutoraldata.zip* su Splunk:

1. Download the `tutorialdata.zip` file. Do not uncompress the file.





1. Creo una query per identificare tutti i tentativi di accesso falliti (failed password).
   La query mostra timestamp (_time), IP di origine (src_ip), utente (user) e motivo del fallimento (reason).



```
source="tutorialdata.zip:*" "Failed password"
| rex "Failed password for (?:(invalid user )?(?P<user>\w+)) from (?P<src_ip>\d{1,3}(\.\d{1,3}){3}
    )"
| eval reason="Failed password"
| table _time, src_ip, user, reason
```

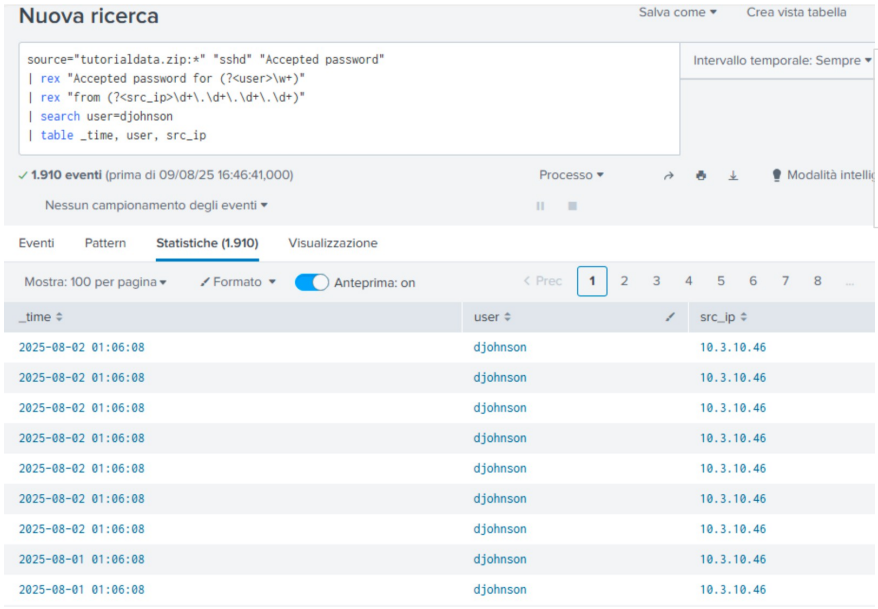
66.506 eventi (prima di 09/08/25 16:21:29,000)

_time	src_ip	user	reason
2025-08-08 01:06:08	46.251.224.66	admin	Failed password
2025-08-08 01:06:08	46.251.224.66	root	Failed password
2025-08-08 01:06:08	46.251.224.66	oracle	Failed password
2025-08-08 01:06:08	46.251.224.66	inet	Failed password
2025-08-08 01:06:08	46.251.224.66	mail	Failed password
2025-08-08 01:06:08	46.251.224.66	local	Failed password
2025-08-08 01:06:08	46.251.224.66	email	Failed password
2025-08-08 01:06:08	148.107.2.20	admin	Failed password
2025-08-08 01:06:08	148.107.2.20	yp	Failed password

Rex: regex per estrarre utente e IP
Eval: per aggiungere la colonna reason, settata a "Failed PW"
Table: per visualizzare i risultati in una tabella

Conclusione: Ci sono 66.506 tentativi di accesso falliti, da diversi nomi utenti e indirizzi IP, segno di un possibile attacco brute force.

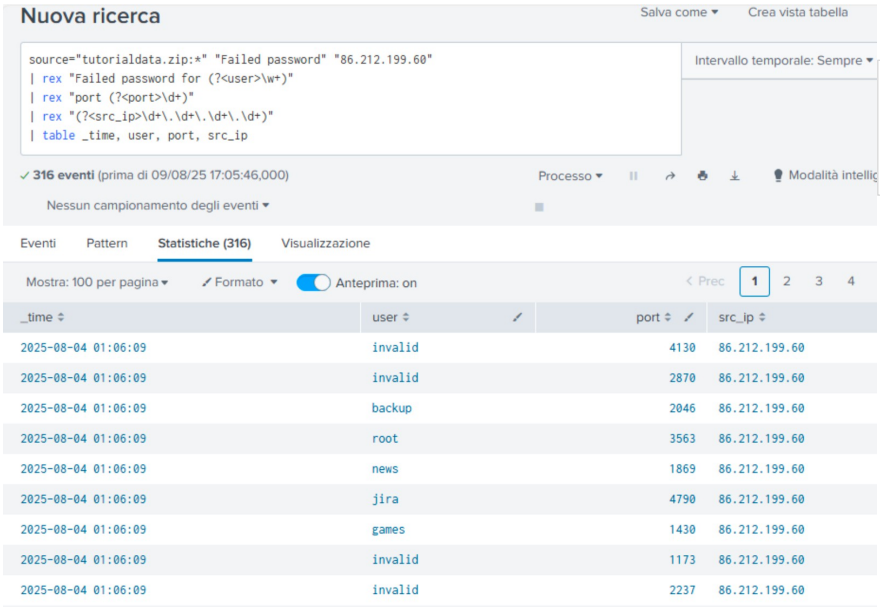
2. Creo una query per trovare tutte le sessioni SSH (sshd) aperte con successo (accepted password).
La query filtra per l'utente "djohnson" e mostra timestamp (_time) e utente (user).



Rex: regex per estrarre utente e IP
Search: per restringere i risultati ai soli eventi dove il campo user = djohnson
Table: per visualizzare i risultati in una tabella

Conclusione: L'utente djohnson (con IP 10.3.10.46) ha effettuato il login più volte nello stesso intervallo di tempo. Il login potrebbe essere stato effettuato tramite una sessione persistente (es. un terminale SSH che non si disconnette) oppure che l'utente si collega da una macchina fissa/da un server specifico senza cambiare IP tra una sessione e l'altra.

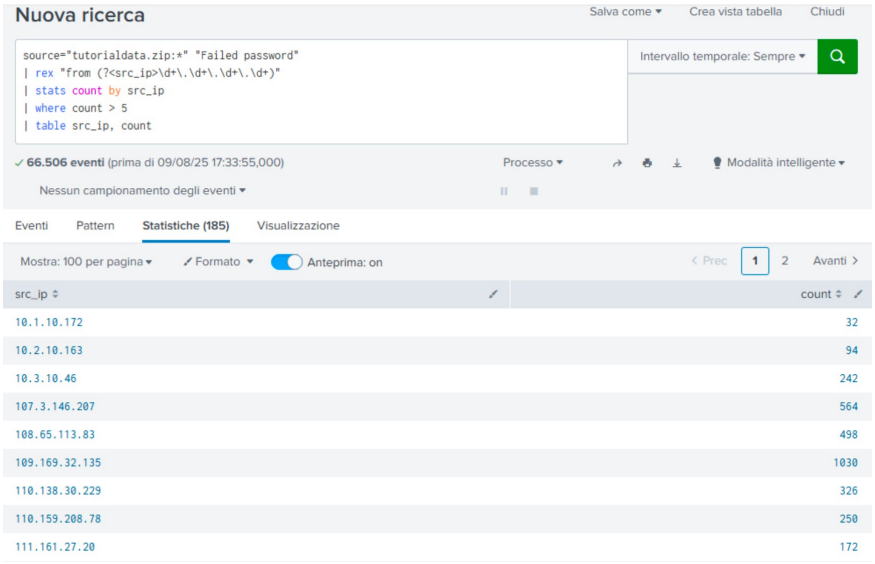
3. Creo una query per trovare tutti i tentativi di accesso falliti provenienti dall'IP 86.212.199.60.
La query mostra timestamp (_time), utente (user) e numero porta (port).



Rex: regex per estrarre utente, IP e porta
Table: per visualizzare i risultati in una tabella

Conclusione: L'IP 82.212.199.60 ha tentato 316 accessi falliti, con diversi nomi utente, segno di un possibile attacco brute force.

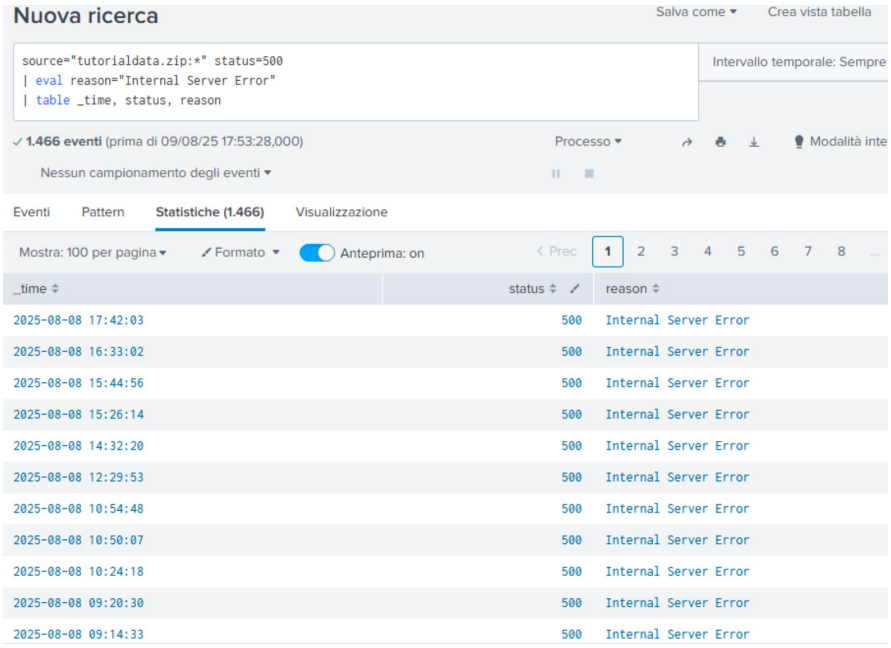
4. Creo una query per identificare gli indirizzi IP che hanno tentato di accedere al sistema più di 5 volte. La query mostra IP (src_ip) e numero di tentativi (count).



Rex: regex per estrarre IP
Stats count by: per contare i tentativi di accesso per ciascun IP
Where: per applicare una condizione
Table: per visualizzare i risultati in una tabella

Conclusione: Molti indirizzi IP hanno tentato più di 400 volte di accedere al sistema, segno di possibili accessi automatizzati o attacchi brute force.

5. Creo una query per trovare tutti gli Internal Server Error (500).



Eval: per aggiungere la colonna reason, settata a “Internal Server Error”
Table: per visualizzare i risultati in una tabella

Conclusione: Ci sono 1.466 Internal Server Error, segno di un problema costante nel sistema (es. malfunzionamento interno del server, errori nelle configurazioni).

Per confermare tutte queste supposizioni, servono analisi più approfondite.