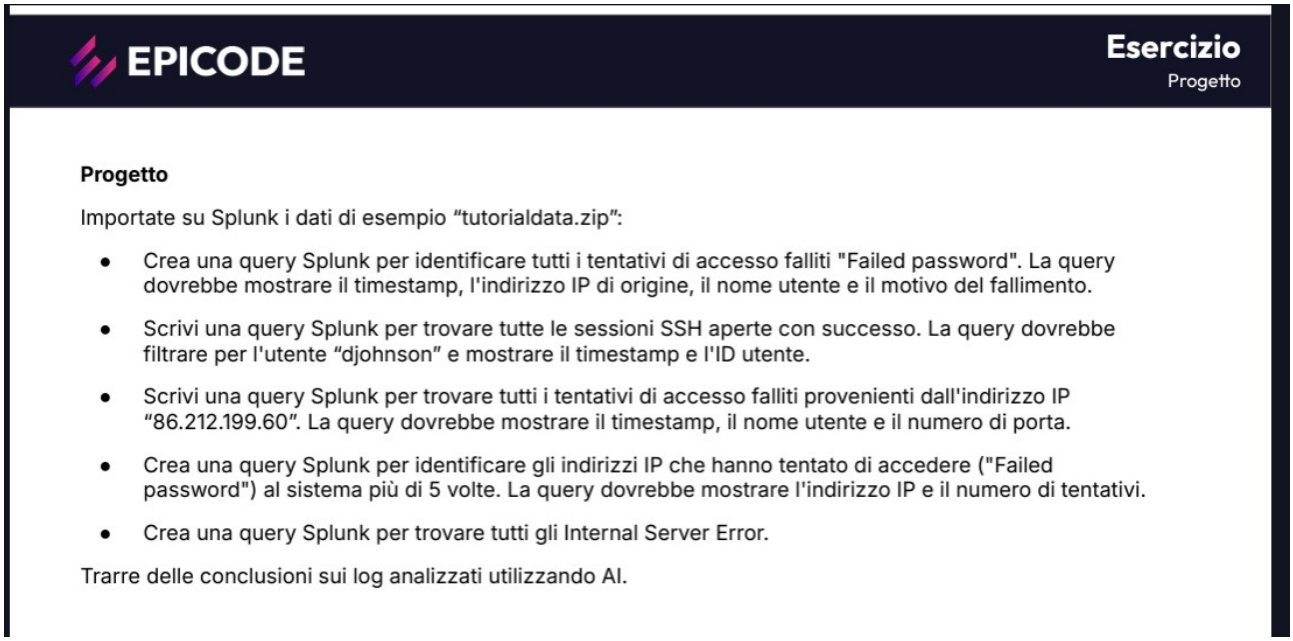
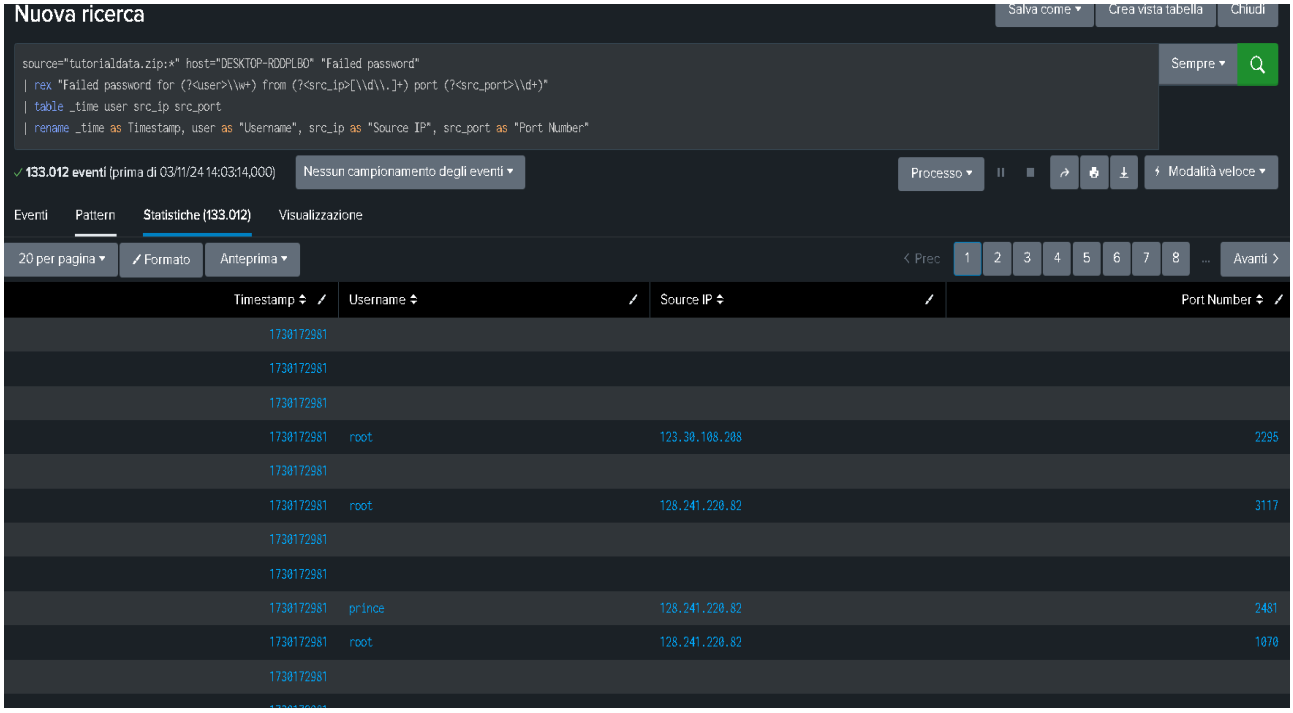
W24D4



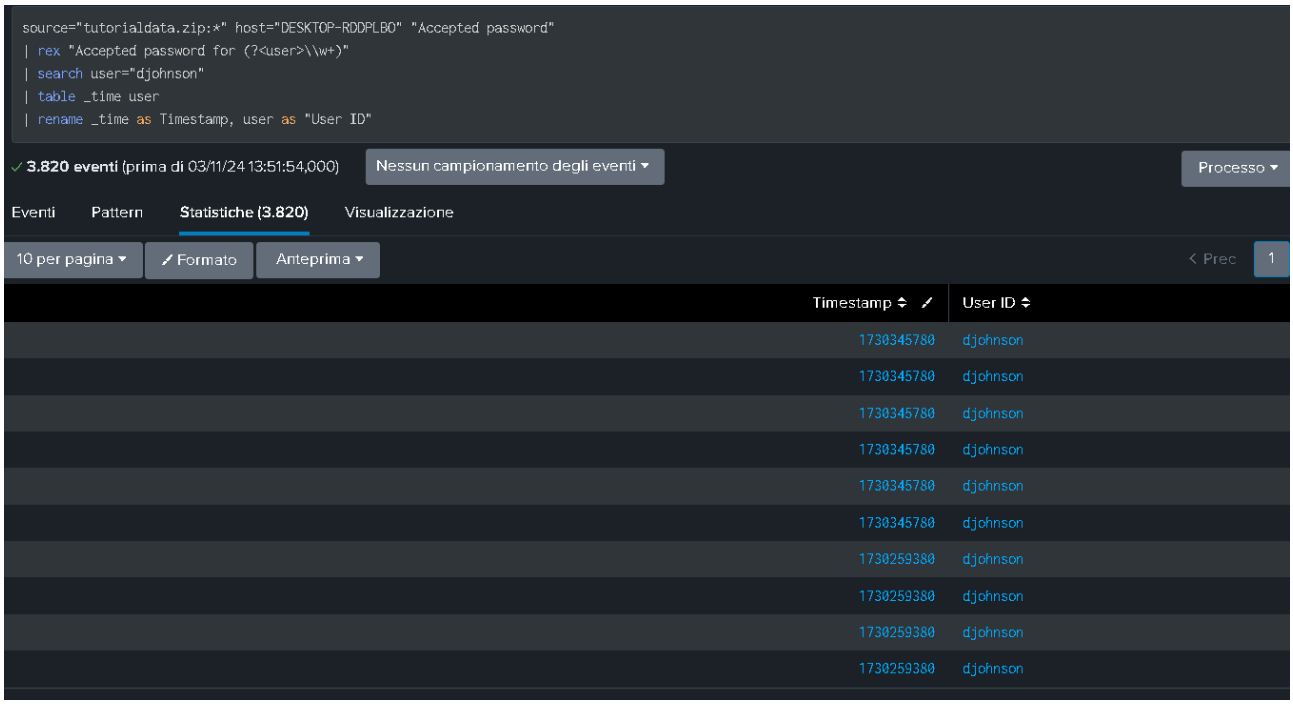
1. Tentativi di accesso falliti ("Failed password")



source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" "Failed password"
| rex "Failed password for (?<user>\\w+) from (?<src_ip>[\\d\\.]+) port (?<src_port>\\d+)"
| table _time user src_ip src_port
| rename _time as Timestamp, user as "Username", src_ip as "Source IP", src_port as "Port Number"

Questa query cerca nell' indice per "Failed password" e restituisce il timestamp, l'indirizzo IP di origine, il nome utente e la porta.

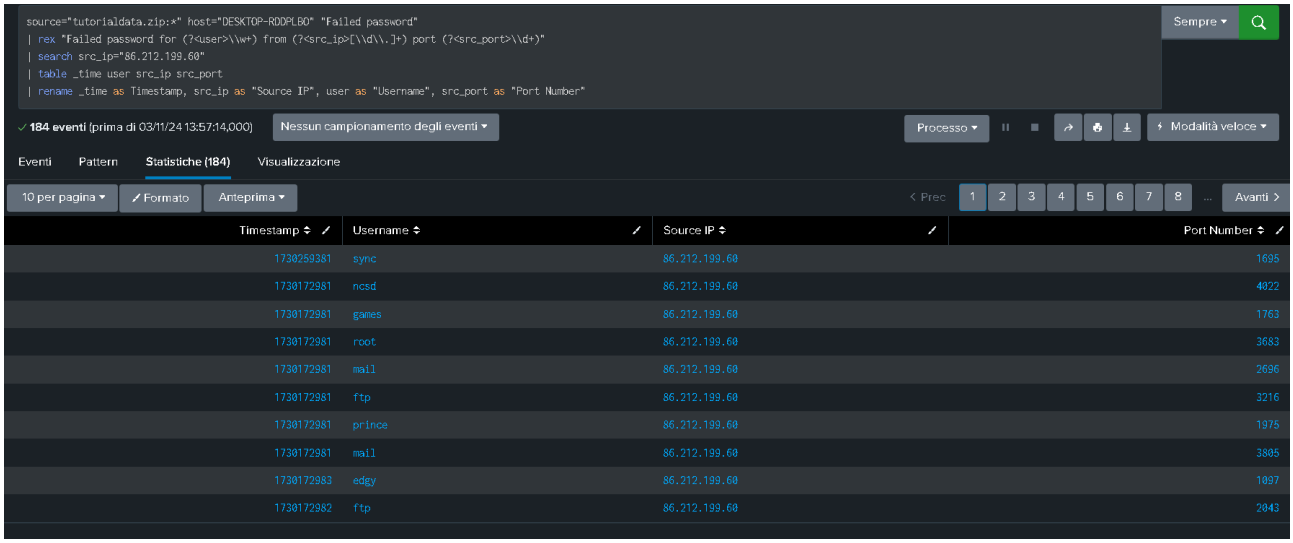
2. Sessioni SSH aperte con successo per l'utente "djohnson"



source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" "Accepted password"
| rex "Accepted password for (?<user>\\w+)"
| search user="djohnson"
| table _time user
| rename _time as Timestamp, user as "User ID"

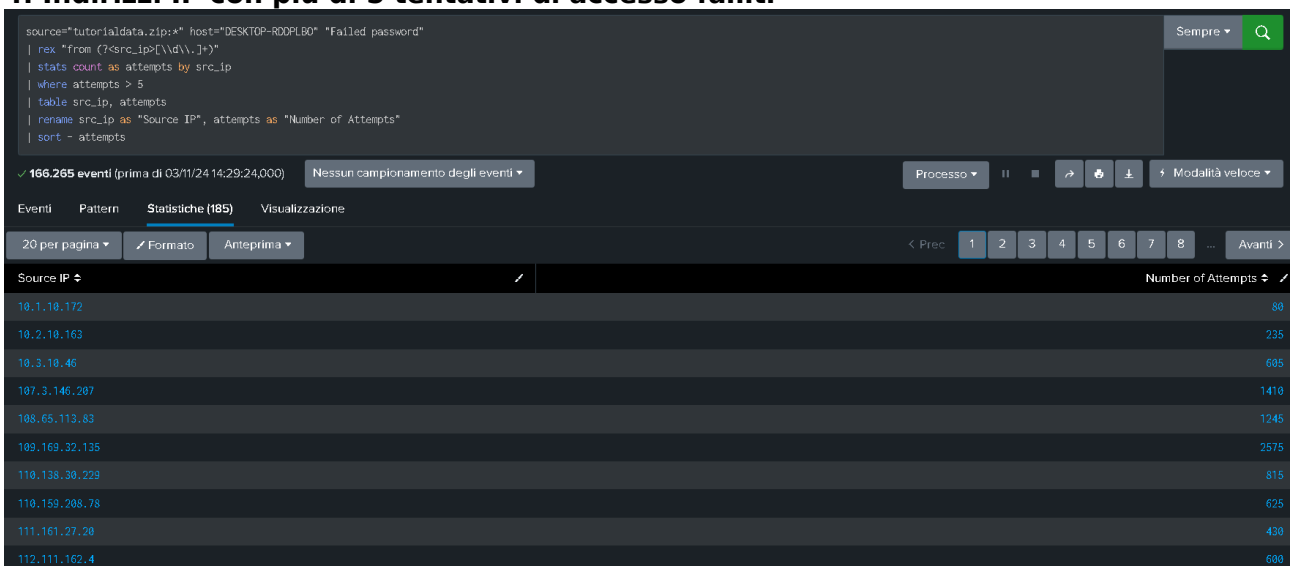
Filtra le sessioni SSH accettate per l'utente specificato e restituisce il timestamp e l'ID utente.

3. Tentativi di accesso falliti dall'indirizzo IP "86.212.199.60"



source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" "Failed password"
| rex "Failed password for (?<user>\\w+) from (?<src_ip>[\\d\\.]+) port (?<src_port>\\d+)"
| search src_ip="86.212.199.60"
| table _time user src_ip src_port
| rename _time as Timestamp, src_ip as "Source IP", user as "Username", src_port as "Port Number"
Questa query cerca tutti i tentativi di accesso falliti provenienti da un IP specifico e mostra il timestamp, il nome utente e il numero di porta.

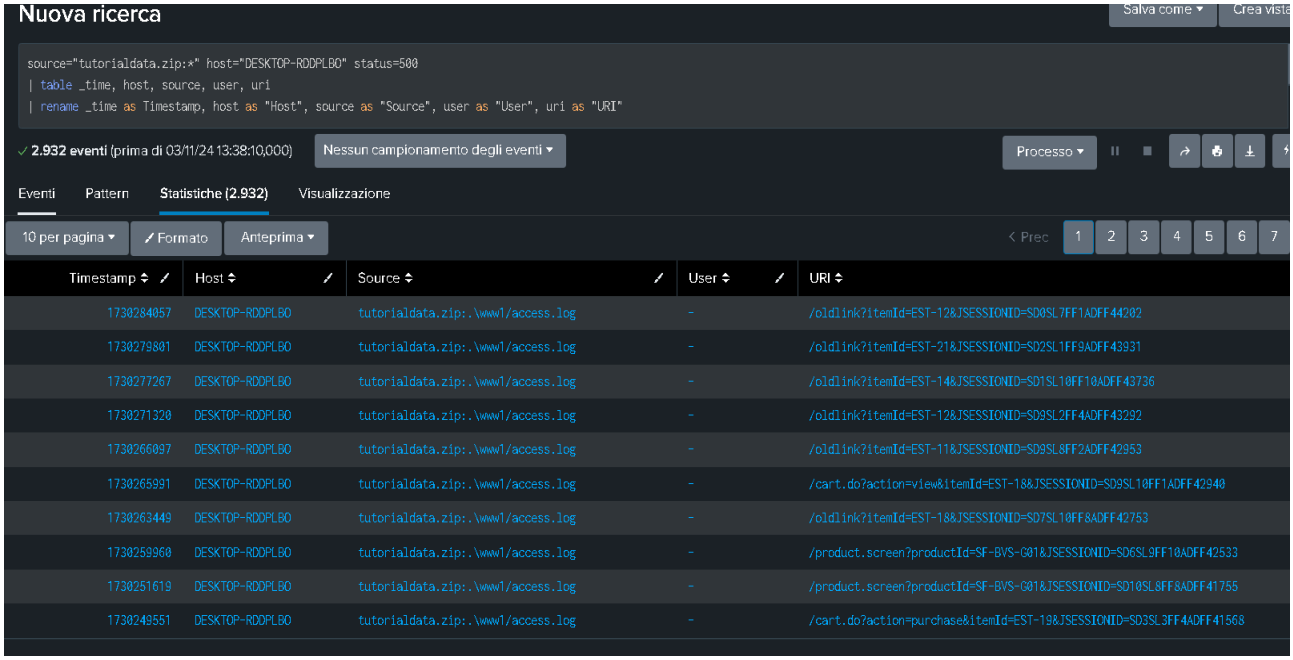
4. Indirizzi IP con più di 5 tentativi di accesso falliti



source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" "Failed password"
| rex "from (?<src_ip>[\\d\\.]+)"
| stats count as attempts by src_ip
| where attempts > 5
| table src_ip, attempts
| rename src_ip as "Source IP", attempts as "Number of Attempts"
| sort - attempts

Conta i tentativi di accesso falliti per ogni indirizzo IP e filtra per quelli con più di 5 tentativi.

5. Errori interni del server (Internal Server Error)



source="tutorialdata.zip:*" host="DESKTOP-RDDPLBO" status=500
| table _time, host, source, user, uri
| rename _time as Timestamp, host as "Host", source as "Source", user as "User", uri as "URI"

Cerca gli errori interni del server e restituisce il timestamp

Conclusioni sui log analizzati :

Analizzando i log, è possibile ottenere informazioni preziose sulla sicurezza e l'affidabilità del sistema. I tentativi di accesso falliti possono indicare attività di forza bruta o attacchi mirati, specialmente se provengono da indirizzi IP con molteplici tentativi. Sessioni SSH aperte con successo per utenti specifici possono evidenziare comportamenti normali o anomali.
Inoltre, l'analisi degli "Internal Server Error" può rivelare problemi ricorrenti con l'infrastruttura o il codice, suggerendo la necessità di miglioramenti o ottimizzazioni. Utilizzando strumenti di intelligenza artificiale, è possibile automatizzare il monitoraggio di questi log per identificare modelli e anomalie in tempo reale, migliorando così la reattività agli attacchi e la stabilità del sistema.

P.S:

Grazie di tutto Prof :) <3