Benchmark W24D4

Cosa è Splunk

Breve descrizione su cosa sia il software, che cosa fa, e il perchè è utile in ambito di cyber security

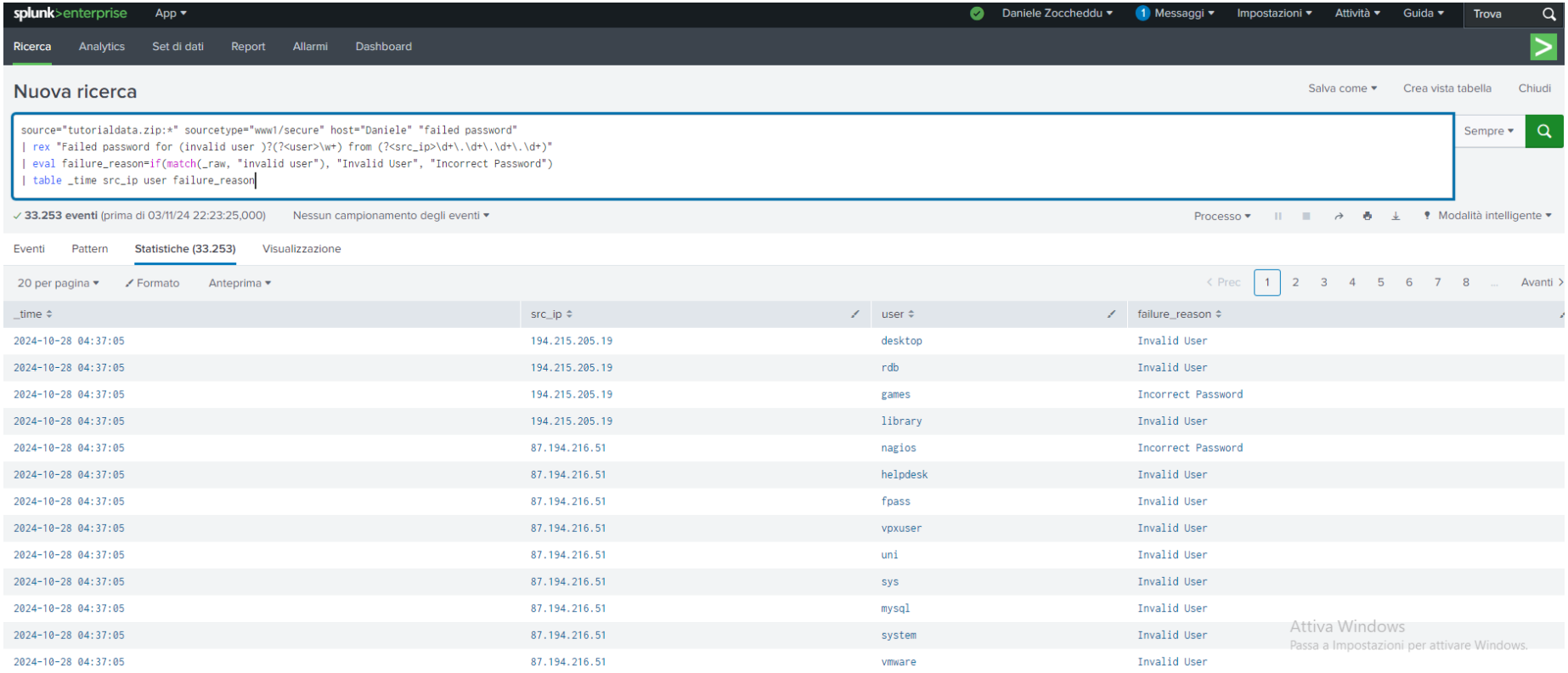
Analisi con query

Dopo aver importato i dati dal file di prova “tutorialdata.zip” posso elaborarli con delle query e trarre conclusioni sui log analizzati utilizzando l'AI.

Identificazione tentativi di accesso falliti

source="tutorialdata.zip:*" sourcetype="www1/secure" host="Daniele" "failed password"
| rex "Failed password for (invalid user)?(?< user>\w+) from (?<src_ip>\d+.\d+.\d+.\d+)"
| eval failure_reason=if(match(_raw, "invalid user"), "Invalid User", "Incorrect Password")
| table _time src_ip user failure_reason

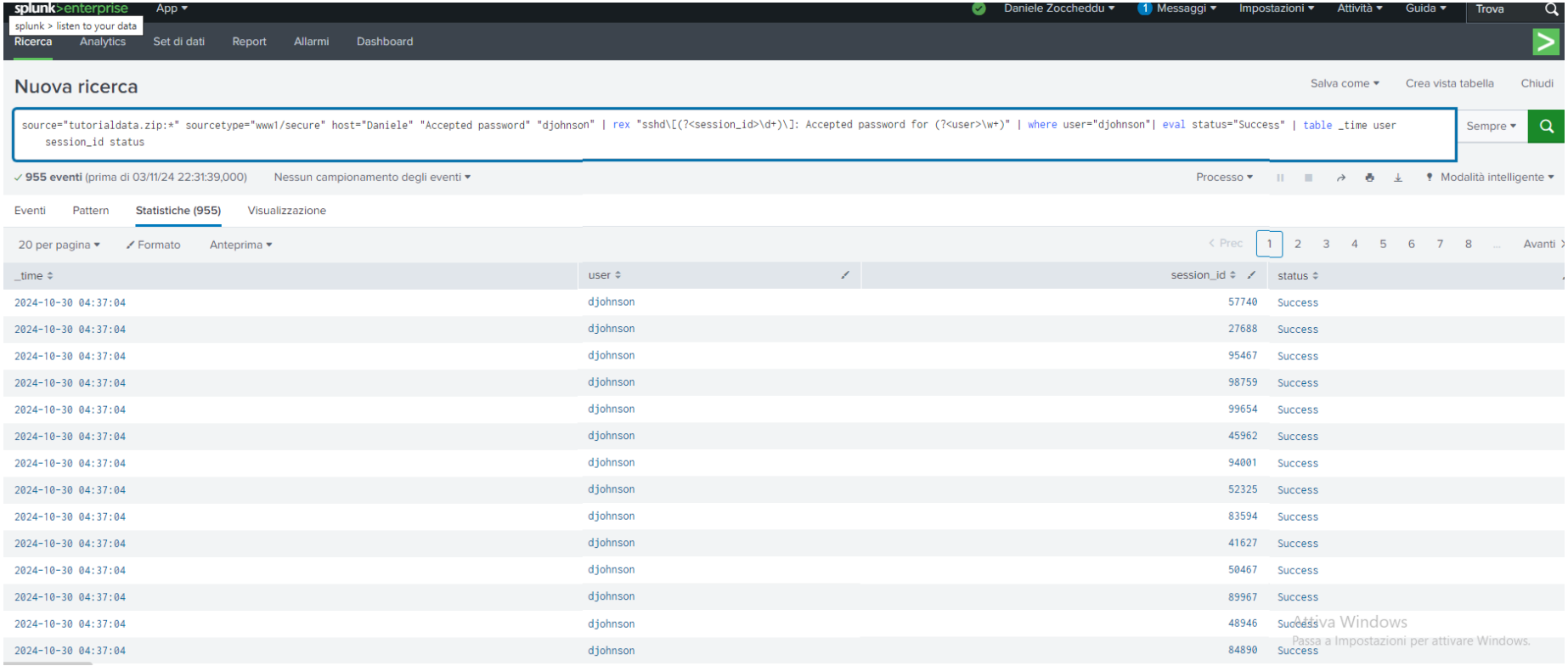
la query mostra il timestamp, il motivo del fallimento,il nome utente e l'indirizzo IP di origine:



Identificazione sessioni SSH aperte con successo

source="tutorialdata.zip:*" sourcetype="www1/secure" host="Daniele" "Accepted password" "djohnson" | rex "sshd[(?<session_id>\d+)]: Accepted password for (?< user>\w+)" | where user="djohnson"| eval status="Success" | table _time user session_id status

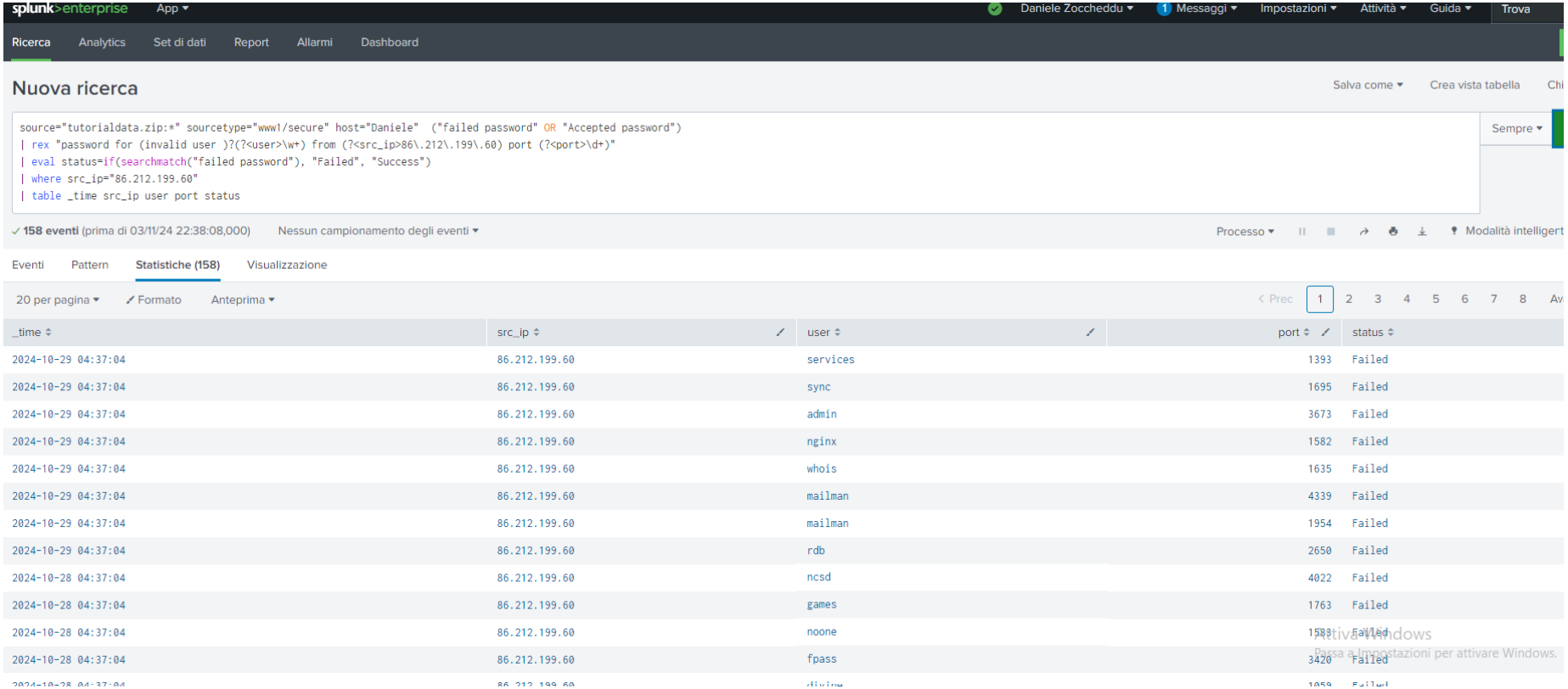
Filtrando per l'utente "djohnson" ottengo le seguenti sessioni:



Ricerca tentativi di accesso falliti

source="tutorialdata.zip:*" sourcetype="www1/secure" host="Daniele" ("failed password" OR "Accepted password")
| rex "password for (invalid user)?(?< user>\w+) from (?< src_ip>86.212.199.60) port (?< port>\d+)"
| eval status=if(searchmatch("failed password"), "Failed", "Success")
| where src_ip="86.212.199.60"
| table _time src_ip user port status

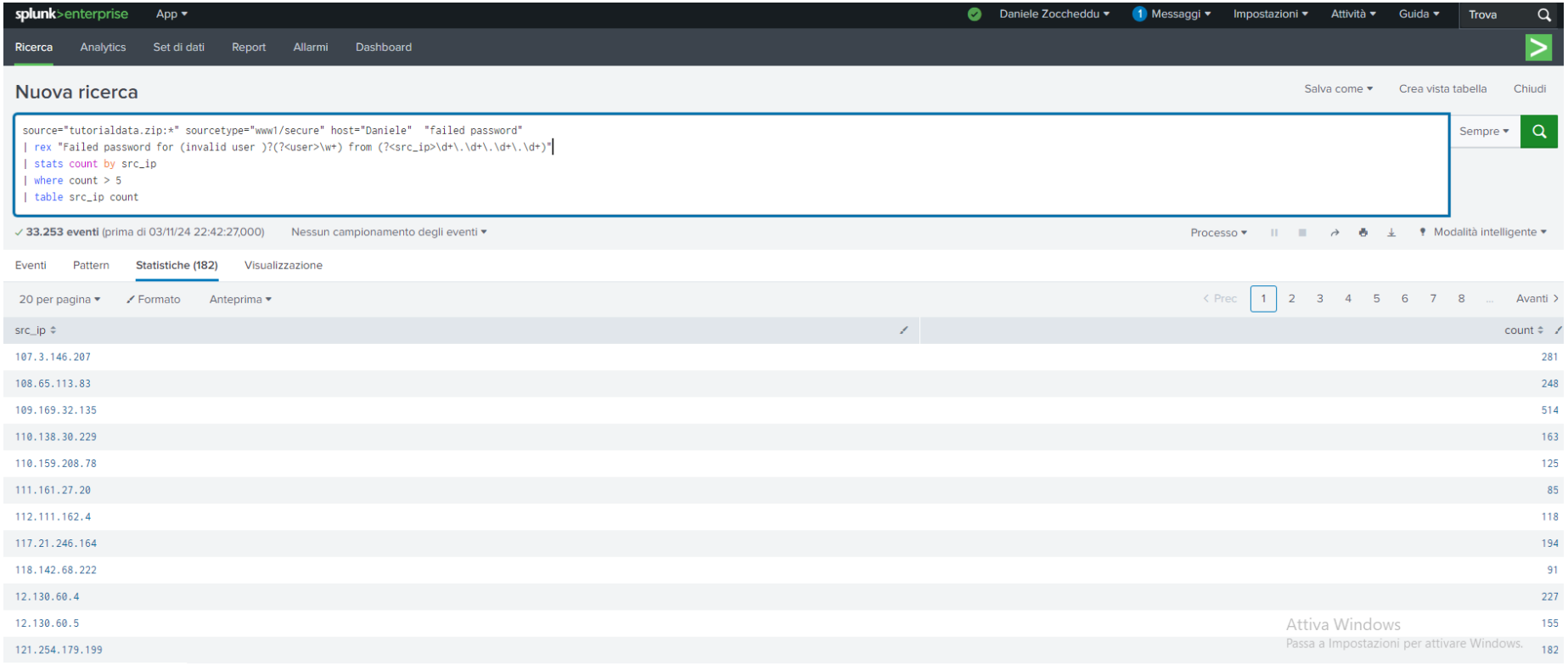
filtrando per l'indirizzo IP "86.212.199.60" ottengo i seguenti tentativi di accesso:



Identificazione indirizzi IP "sospetti"

Solitamente quando ci sono multipli tentativi errati di accesso da parte di uno stesso indirizzo IP in un sistema (fallendo di inserire correttamente la password) questo è indice di un possibile tentativo di bruteforcing. Questa query da gli indirizzi IP e il numero di tentativi di quelli che provano senza successo ad accedere per più di 5 volte:

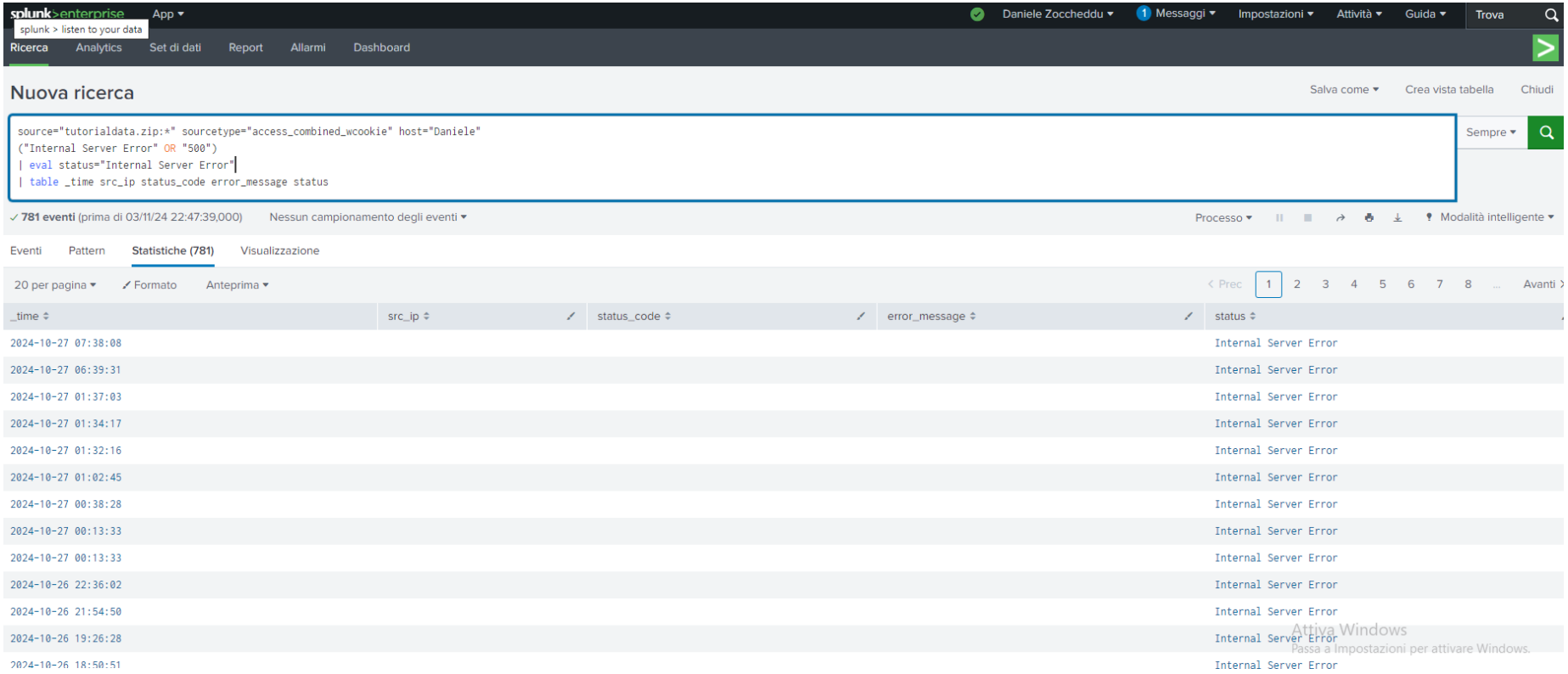
source="tutorialdata.zip:*" sourcetype="www1/secure" host="Daniele" "failed password"
| rex "Failed password for (invalid user)?(?< user>\w+) from (?<src_ip>\d+.\d+.\d+.\d+)"
| stats count by src_ip
| where count > 5
| table src_ip count



Ricerca Internal Server Error

Gli Internal Server Error sono errori generici che indicano che il server ha incontrato una condizione imprevista che gli ha impedito di soddisfare una richiesta.

source="tutorialdata.zip:*" sourcetype="access_combined_wcookie" host="Daniele"
("Internal Server Error" OR "500")
| eval status="Internal Server Error"
| table _time src_ip status_code error_message status



Conclusione tratte analizzando i log con la AI

Tentativi di Accesso Falliti:

Nei log relativi ai tentativi di accesso falliti ("Failed password"), è emerso che diversi indirizzi IP hanno ripetutamente tentato di accedere al sistema senza successo. Questi comportamenti potrebbero indicare:

- **Attività di forza bruta**: IP che eseguono numerosi tentativi falliti possono indicare tentativi di forza bruta, in cui un attaccante cerca di indovinare le credenziali.
- **Potenziale abuso di credenziali**: Alcuni utenti specifici possono essere presi di mira ripetutamente, suggerendo che l'attaccante abbia alcune informazioni preliminari sulle credenziali valide.

Accessi SSH di Successo per Utenti Specifici:

Le sessioni SSH aperte con successo dall'utente "djohnson" hanno mostrato accessi regolari e legittimi. Tuttavia, è importante considerare:

- **Monitoraggio degli utenti privilegiati**: L'account "djohnson" potrebbe essere amministrativo, quindi è essenziale monitorare questi accessi per individuare attività anomale, come connessioni fuori orario o da IP insoliti.

Tentativi di Accesso da un IP Specifico:

Analizzando i tentativi di accesso falliti provenienti dall'indirizzo IP **86.212.199.60**, è stato riscontrato un comportamento ripetitivo che suggerisce:

- **Attività sospette o dannose**: L'IP potrebbe far parte di un attacco mirato, con tentativi di accesso ripetuti verso utenti specifici e su porte definite.
- **Inserimento nella blacklist**: Si potrebbe considerare l'aggiunta di questo IP alla blacklist o l'implementazione di un sistema di rilevamento delle intrusioni (IDS) per prevenire futuri tentativi.

Indirizzi IP con Più di 5 Tentativi di Accesso Falliti:

Gli indirizzi IP con oltre 5 tentativi di accesso falliti rappresentano una potenziale minaccia. I modelli osservati indicano:

- **Potenziale attacco di forza bruta distribuita**: Se più IP eseguono tentativi ripetuti, potrebbe trattarsi di un attacco coordinato.
- **Segmentazione degli attacchi**: In alcuni casi, tali attacchi possono essere distanziati nel tempo per evitare il rilevamento; è fondamentale monitorare continuamente questi IP e implementare sistemi di difesa come firewall e strumenti di prevenzione delle intrusioni.

Errori di Server Interno (Internal Server Error):

Gli errori di tipo "Internal Server Error" (codice 500) possono indicare problemi nei servizi interni o nelle applicazioni web. Questi errori sono spesso associati a:

- **Problemi di configurazione o codice**: Gli errori 500 sono comunemente causati da configurazioni errate o problemi nel codice dell'applicazione; è cruciale che il team di sviluppo esamini i log per individuarne la causa.

- **Possibili vettori di attacco**: Gli errori 500, se correlati a input dell’utente, possono esporre vulnerabilità sfruttabili per attacchi di iniezione o altre tecniche di exploit.

Monitorare costantemente questi eventi e adottare misure preventive aiuta a mantenere la sicurezza del sistema e prevenire intrusioni o disservizi.