PROGETTO

Analisi del Malware e Splunk

M6W24-D4

28 / 02 / 2025

Cybersecurity Analyst

Analisi del Malware e Splunk

TEAM 4 – M.E.M. Splunkers
Matteo Madonia, Emanuele Leonzio, Marco Caobianco

SOMMARIO PROGETTO

1. **Traccia Progetto** Pag. 2
   1.1 Progetto Pag. 2

2. **Premessa e preparazione al laboratorio** Pag. 2
   2.1 Cos'è Splunk? Pag. 2
   2.2 Come funziona Splunk Pag. 2
   2.3 Quali sono le componenti principali di Splunk Pag. 3
   2.4 Preparazione del laboratorio Pag. 3

3. **Svolgimento del progetto** Pag. 5
   3.1 Importazione della cartella dati "tutorialdata.zip" in Splunk Pag. 5
   3.2 Query in Splunk, ricerche di Dati Pag. 11
      3.2.1 Query 1 Pag. 11
      3.2.2 Query 2 Pag. 13
      3.2.3 Query 3 Pag. 14
      3.2.4 Query 4 Pag. 15
      3.2.5 Query 5 Pag. 16

SOMMARIO IMMAGINI

1. Immagine 1 – Home Page Splunk Pag. 3
2. Immagine 2 – Cartella tutorialdata.zip sul Desktop Pag. 4
3. Immagine 3 – Home Page Splunk sezione aggiungi dati Pag. 5
4. Immagine 4 – Sezione aggiungi dati – carica in Splunk Pag. 5
5. Immagine 5 – Sezione carica – seleziona dati in Splunk Pag. 6
6. Immagine 6 – Upload file in Splunk Pag. 6
7. Immagine 7 – Apertura file in Splunk Pag. 7
8. Immagine 8 – Seleziona file dopo il caricamento in Splunk Pag. 7
9. Immagine 9 – File caricato in Splunk Pag. 7
10. Immagine 10 – Impostazioni di input in Splunk Pag. 8
11. Immagine 11 – Verifica impostazioni input in Splunk Pag. 9
12. Immagine 12 – Pagina di verifica in Splunk Pag. 9
13. Immagine 13 – Avvia ricerca in Splunk Pag. 10
14. Immagine 14 – Visualizzazione eventi in Splunk Pag. 10
15. Immagine 15 – Campo ricerca in Splunk Pag. 11
16. Immagine 16 – eventi query 1 Pag. 11
17. Immagine 17 – eventi query 1 con AI Pag. 12
18. Immagine 18 – eventi query 2 Pag. 13
19. Immagine 19 – eventi query 3 Pag. 14
20. Immagine 20 – eventi query 4 Pag. 15
21. Immagine 21 – eventi query 5 Pag. 16

1. Traccia progetto

1.1 Progetto

Importate su Splunk i dati di esempio “tutorialdata.zip”:

- 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.

- 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.

- 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.

- 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.

- Crea una query Splunk per trovare tutti gli Internal Server Error. Trarre delle conclusioni sui log analizzati utilizzando AI.

2. Premessa e preparazione laboratorio

2.1 Cos’è Splunk?

Splunk è una piattaforma software utilizzata per raccogliere, analizzare e visualizzare dati di log generati da applicazioni, dispositivi e infrastrutture IT. È particolarmente usata in ambito di **cybersecurity**, monitoraggio delle prestazioni e analisi dei dati in tempo reale.

Splunk consente di:

- **Collezionare e indicizzare** dati strutturati e non strutturati da diverse fonti (log di sistema, eventi di rete, sensori IoT, ecc.).
- **Effettuare ricerche e analisi** su grandi volumi di dati utilizzando un linguaggio di query chiamato **SPL (Search Processing Language)**.
- **Creare dashboard e report** per la visualizzazione interattiva dei dati.
- **Impostare avvisi automatici** basati su condizioni specifiche.

In ambito **cybersecurity**, Splunk è spesso utilizzato come **SIEM (Security Information and Event Management)** per rilevare minacce e rispondere agli incidenti di sicurezza.

2.2 Come funziona Splunk?

1. Raccolta Dati: Splunk raccoglie dati da diverse fonti (server, dispositivi di rete, applicazioni, ecc.).
2. Indicizzazione Dati: I dati raccolti vengono indicizzati per consentire ricerche rapide e analisi.
3. Parsing dei Dati: Durante l'indicizzazione, Splunk esegue il parsing dei dati, ossia l'analisi e la trasformazione dei dati grezzi in campi strutturati.
4. Ricerca e Analisi: Gli utenti possono eseguire ricerche sui dati indicizzati utilizzando query per estrarre informazioni utili.
5. Visualizzazione Dati: Splunk permette di creare dashboard, grafici e report per visualizzare i risultati delle analisi.

2.3 Quali sono le componenti principali di Splunk?

Host:

L'host è il nome del sistema o del dispositivo da cui provengono i dati.

Source:

La source è il percorso o il file specifico da cui i dati sono stati raccolti.

Sourcetype:

Il sourcetype è una categorizzazione del formato dei dati raccolti. Definisce come i dati devono essere interpretati da Splunk.

Parsing:

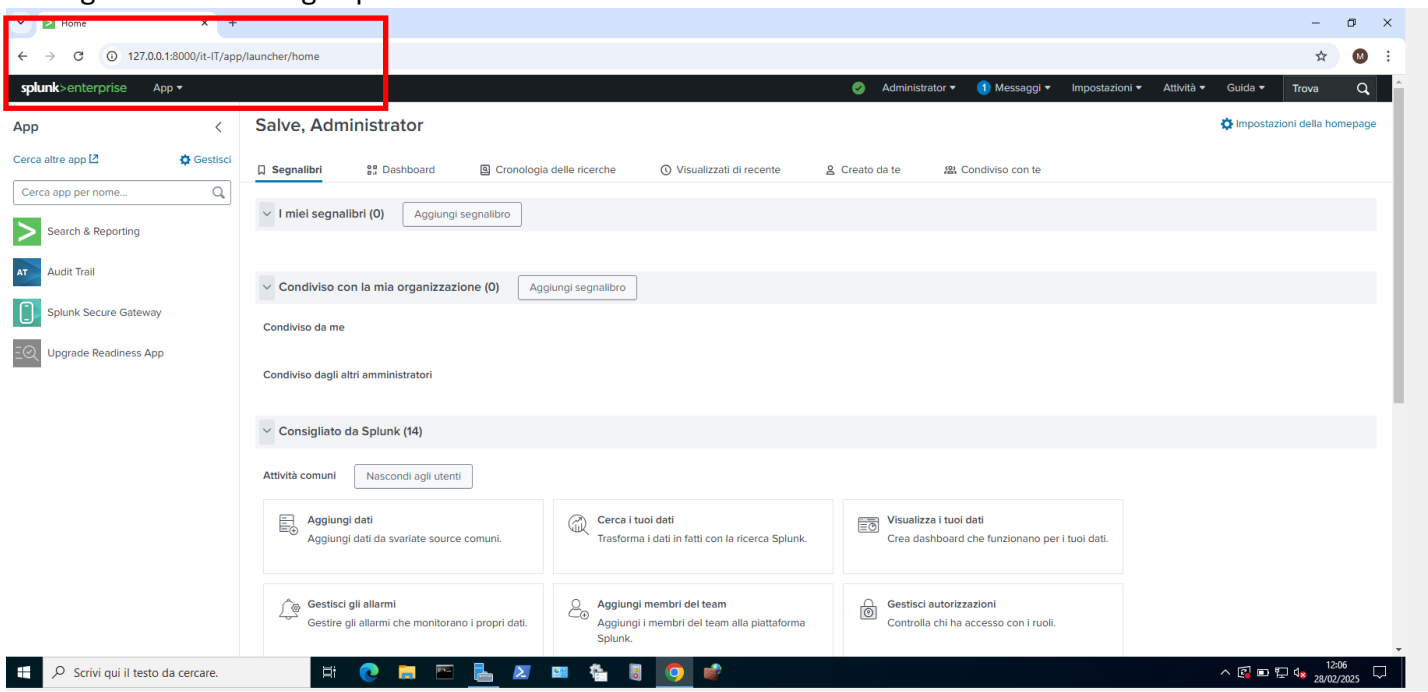
Il parsing è il processo di analisi dei dati grezzi per estrarre e strutturare le informazioni in campi definiti, come timestamp, indirizzi IP, URL, ecc. ○ Esempio: Estrazione di campi da un log di accesso Nginx come timestamp, metodo HTTP, URL richiesto, codice di stato.

2.4 Preparazione del laboratorio

Al fine di iniziare correttamente lo svolgimento di questo progetto, la piattaforma web di Splunk deve essere stata preventivamente installata e funzionante (versione Trial); all'interno di questo laboratorio la stessa è stata installata su Windows Server 2022 e la troviamo digitando nel campo URL l'indirizzo di loopback 127.0.0.1 alla porta 8000; fare riferimento al laboratorio M6W24-D1

Ecco come appare la sua Home Page dopo aver effettuato il login:

Immagine 1 – Home Page Splunk

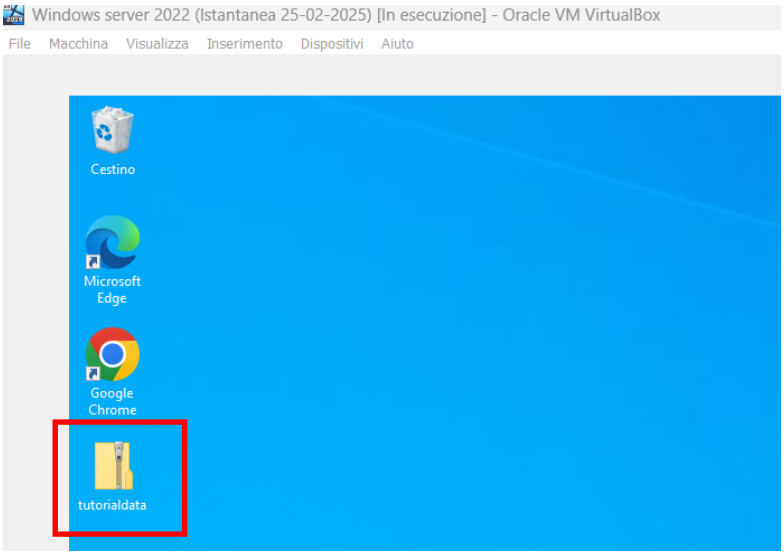


Una volta raggiunta l'Home Page, Splunk è pronto per svolgere il suo lavoro.

Per lo svolgimento di questo laboratorio è richiesto un import di dati predefiniti contenuti nella cartella "tutorialdata.zip", scaricabile gratuitamente dal sito ufficiale di Splunk (made by CISCO). Questa cartella di dati è stata messa a disposizione da CISCO per agevolare gli utenti alle prime armi, per conoscere a fondo il tool, metodi di ricerca dati ecc. ecc.

In questo caso il download era già stato effettuato per lo svolgimento del progetto M6W24-D1, quindi lo trovo già presente sul Desktop di Windows Server 2022, come da immagine di seguito:

Immagine 2 – Cartella tutorialdata.zip sul Desktop

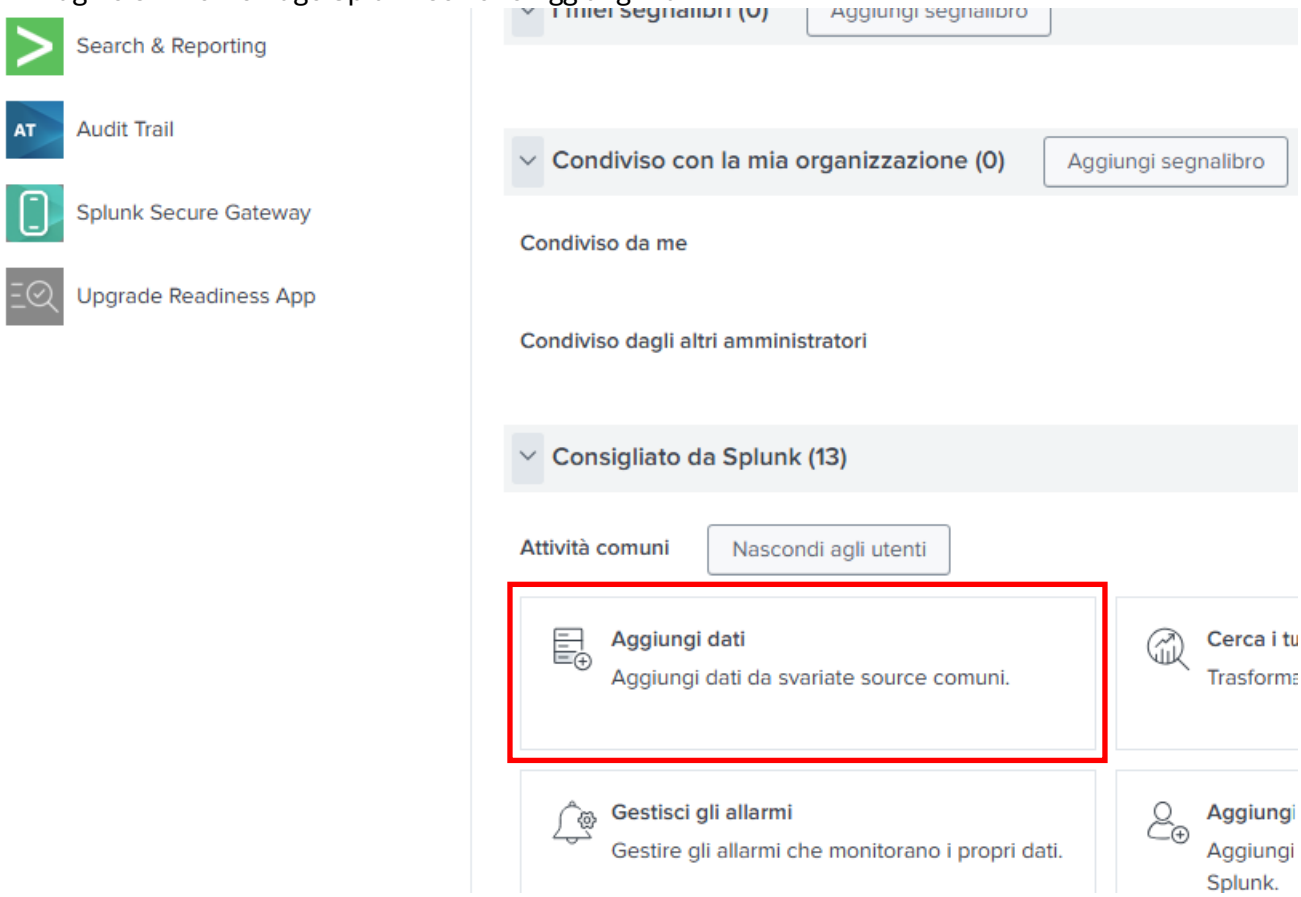


3 Svolgimento del Progetto

3.1 Importazione della cartella dati "tutorialdata.zip" in Splunk

Torniamo ora nella home page di Splunk, e carichiamo il file tutorialdata.zip (nota bene: non bisogna estrarlo ma caricarlo con l'estensione .zip), cliccando sulla sezione "aggiungi dati"

Immagine 3 – Home Page Splunk sezione Aggiungi Dati

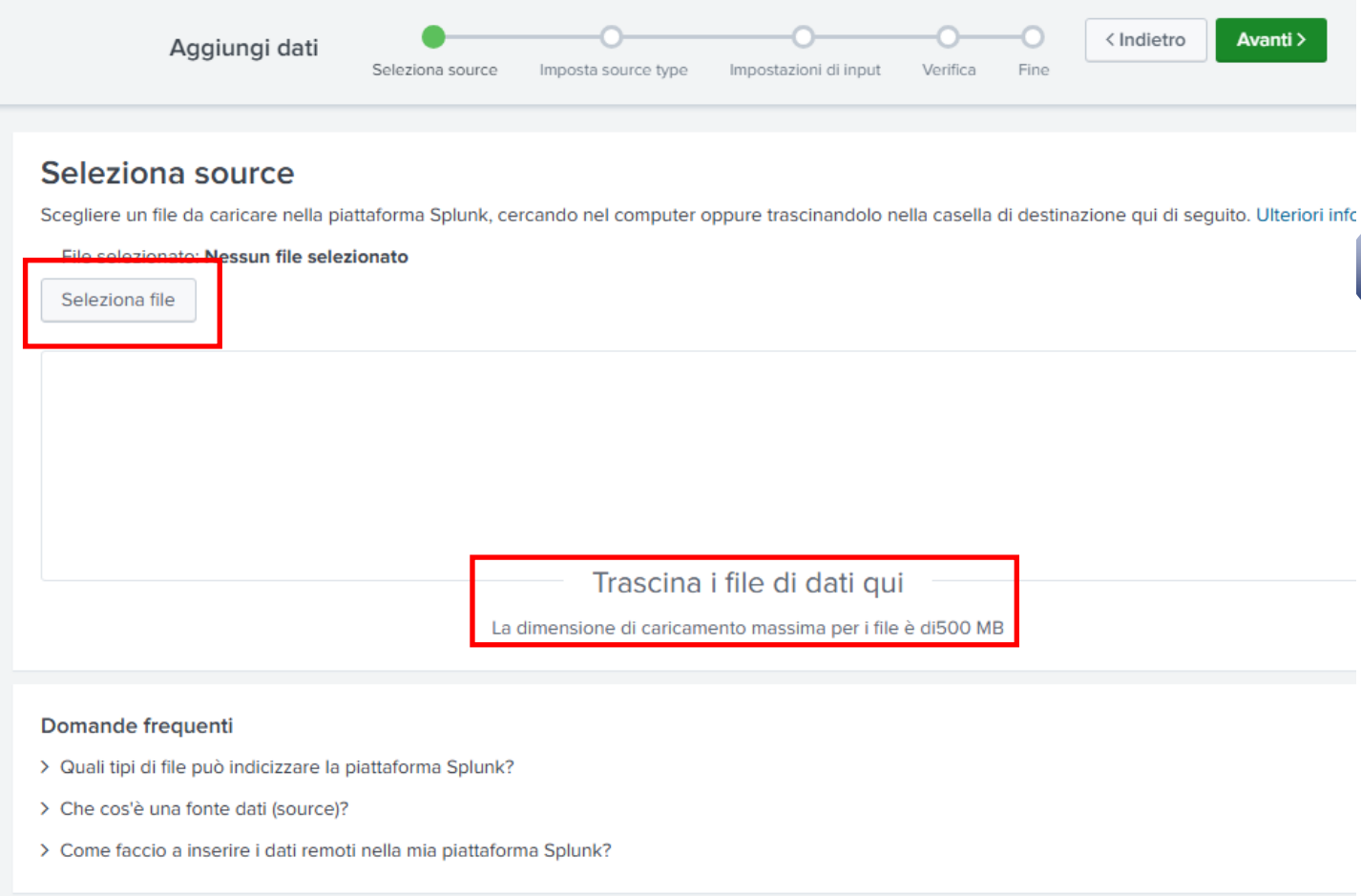


Cliccare ora sulla sezione "carica"

Immagine 4 – Sezione aggiungi dati – carica in Splunk

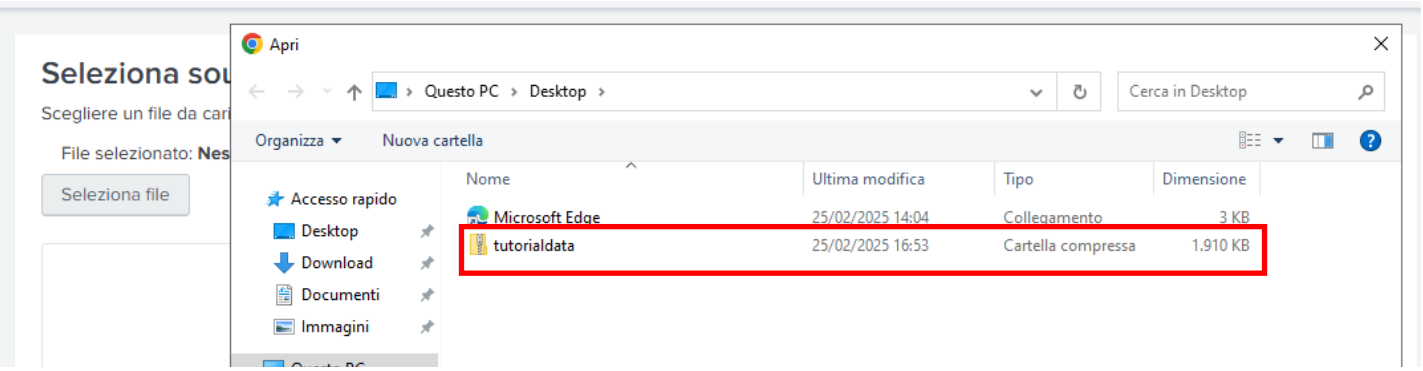
Per caricare “tutorialdata.zip” è necessario cliccare su “Seleziona file” oppure trascinare direttamente la cartella nell’apposita sezione indicata:

Immagine 5 – Sezione carica – seleziona dati in Splunk



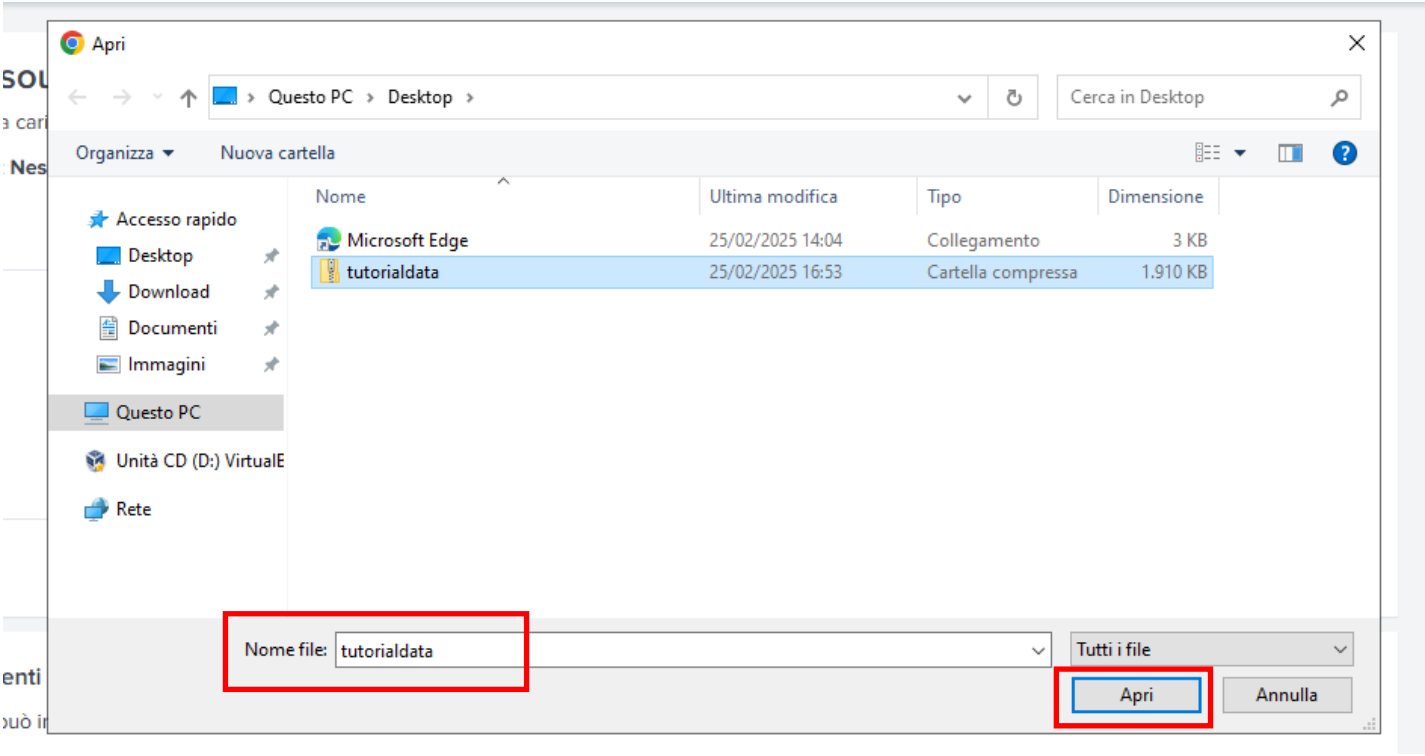
Selezionare il file.zip da prendere in esame

Immagine 6 – Upload file in Splunk



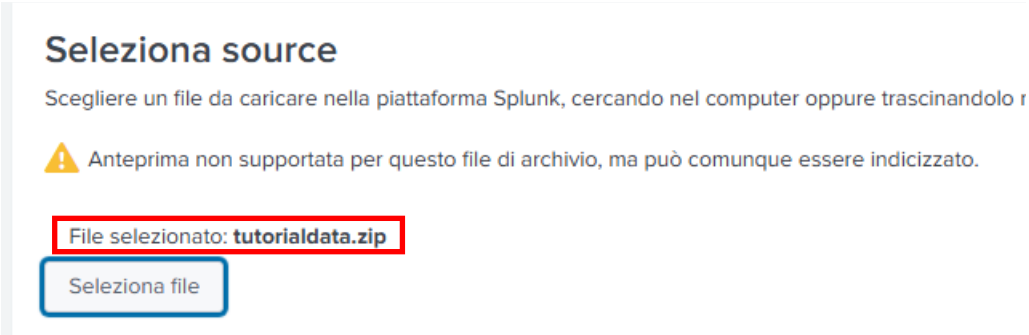
Cliccare su “Apri”

Immagine 7 – Apertura file in Splunk



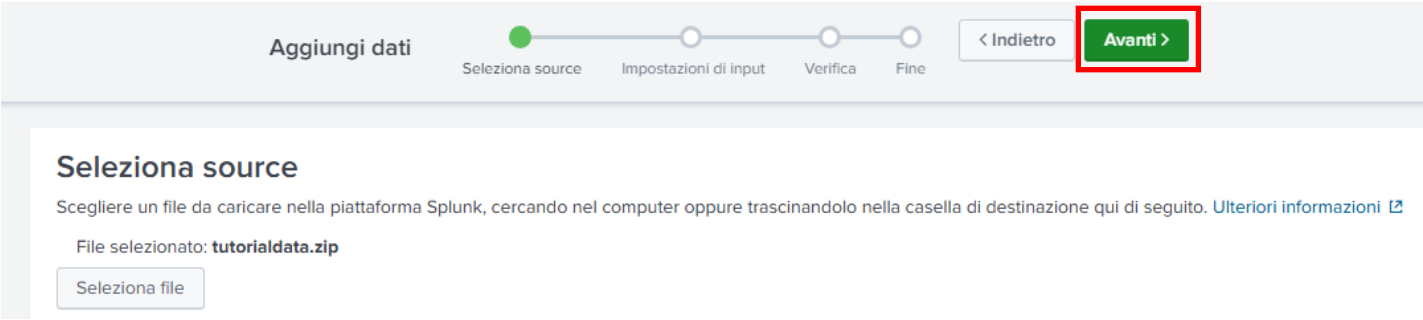
Una volta aperto il file, questa è la schermata che dobbiamo avere; il file è stato correttamente selezionato e aperto, quasi pronto per l’importazione

Immagine 8 – Seleziona file dopo il caricamento in Splunk



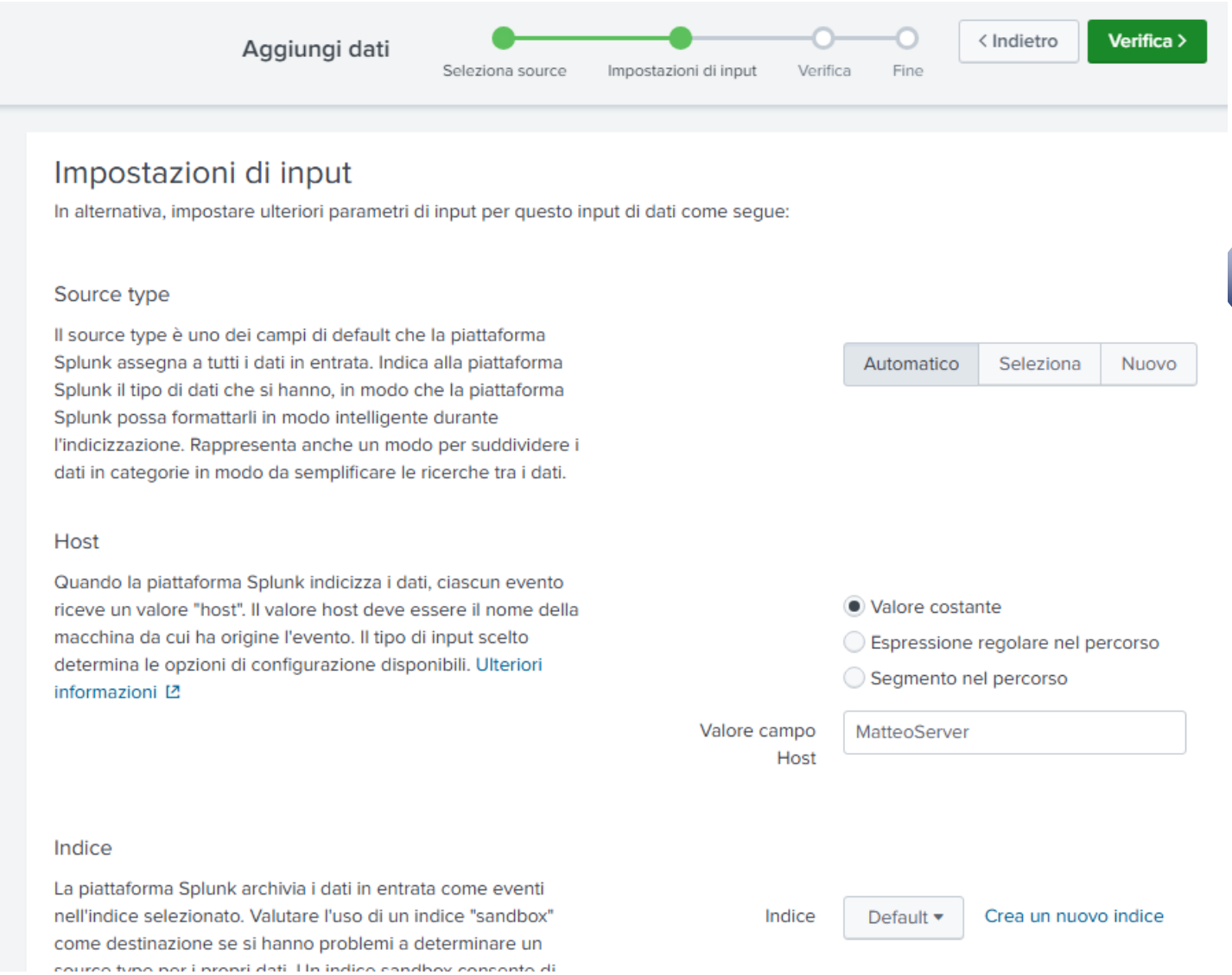
Cliccare ora su “Avanti”

Immagine 9 – File caricato in Splunk



Una volta cliccato su avanti, Splunk ci mostrerà questa schermata:

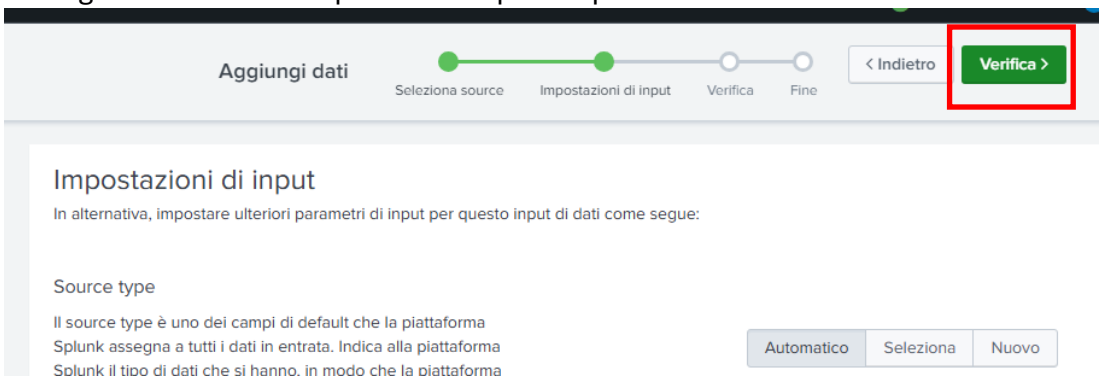
Immagine 10 – Impostazioni di input in Splunk



Splunk, per il suo corretto funzionamento e futura indicizzazione dei dati, si basa su settaggi molto importarti da effettuare prima di importare il file di dati analizzare, in quanto ogni file è a se e può avere origini differenti; esso si compone di Host, Sourcetype e Index, che in questo caso provvediamo a lasciare di default. Per garantire a Splunk un corretto “Parsing” dei dati per la creazione dei campi d’indicizzazione, è necessario quindi settare correttamente il tool.

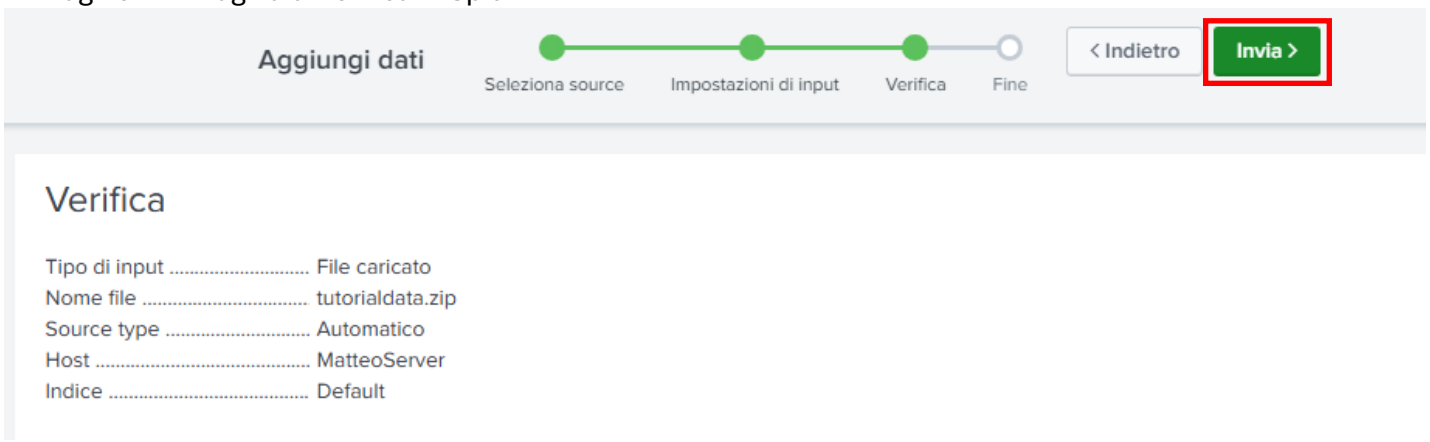
Procedere quindi cliccando su “Verifica”

Immagine 11 – Verifica impostazioni input in Splunk



Dopo aver cliccato su “Verifica”, questa è la schermata che ci verrà proposta:

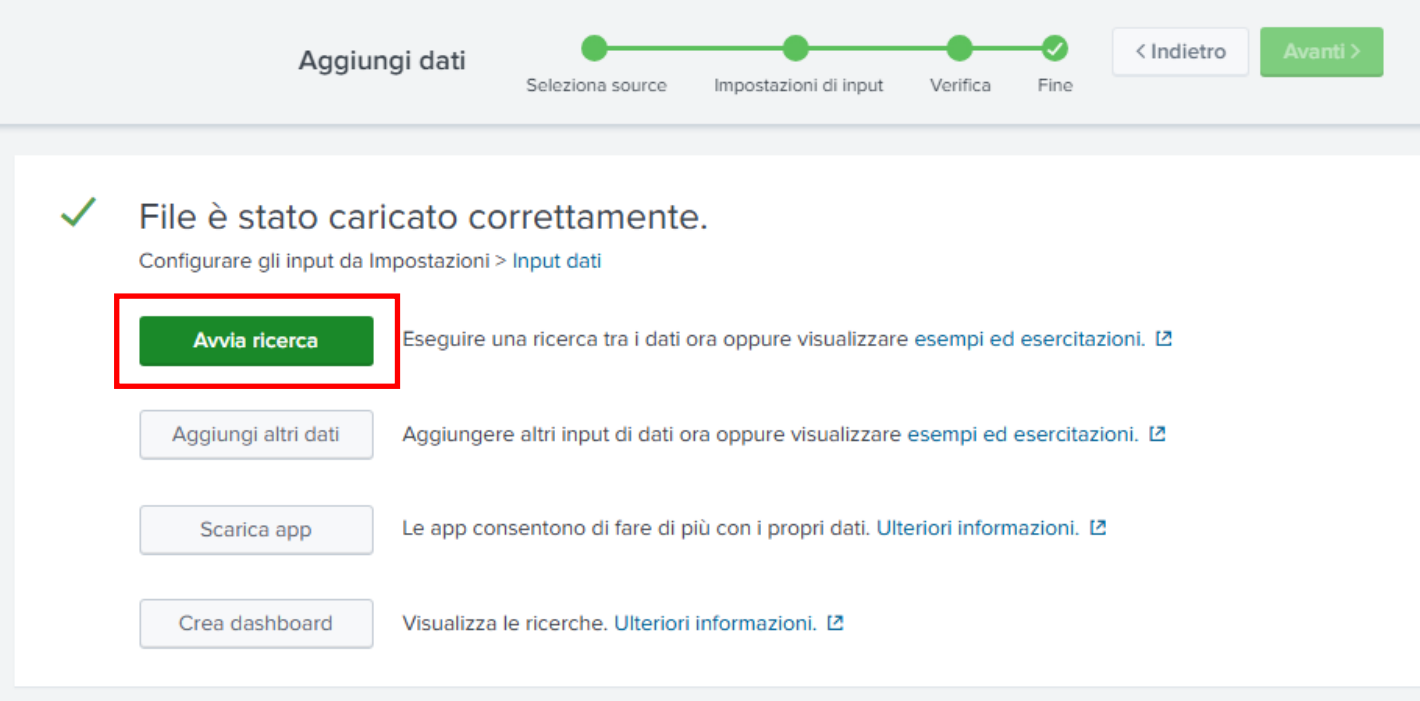
Immagine 12 – Pagina di verifica in Splunk



Cliccando su “Invia”, finalmente importiamo in Splunk il file dati “tutorialdata.zip” e il tool risulterà finalmente operativo.

A seguito di "Invia" di seguito la schermata che dobbiamo ottenere:

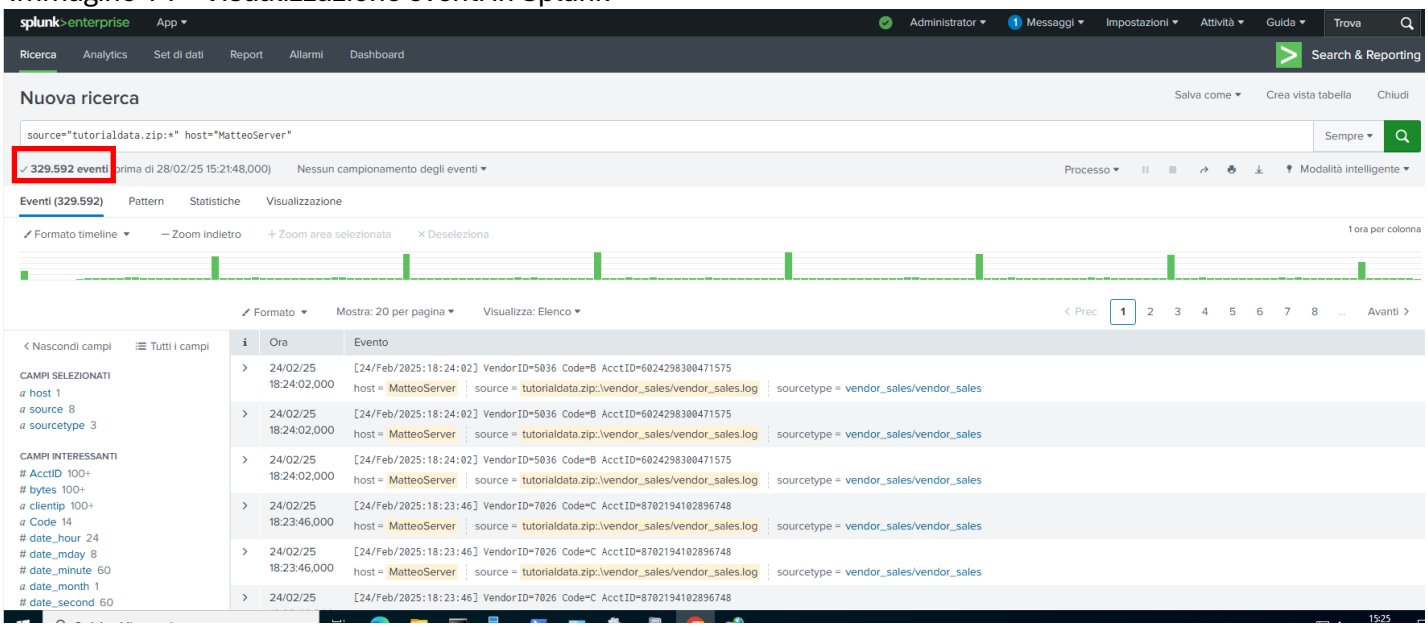
Immagine 13 – Avvia ricerca in Splunk



Procedere ora cliccando su "Avvia ricerca" per essere operativi al 100% e iniziare le ricerche di dati tramite apposite Query (SPL) di Splunk, per quanto richiesto in questo laboratorio.

A seguito dell'avvia ricerca, Splunk ci propone la sua home page, comprensiva di tutti i dati già elaborati e contenuti nel file da noi caricati "tutorialdata.zip"; in questa immagine è possibile notare il numero di eventi che Splunk, dopo l'elaborazione della cartella .zip, ha messo a nostra disposizione per iniziare le ricerche richieste; sono presenti 329.592 eventi

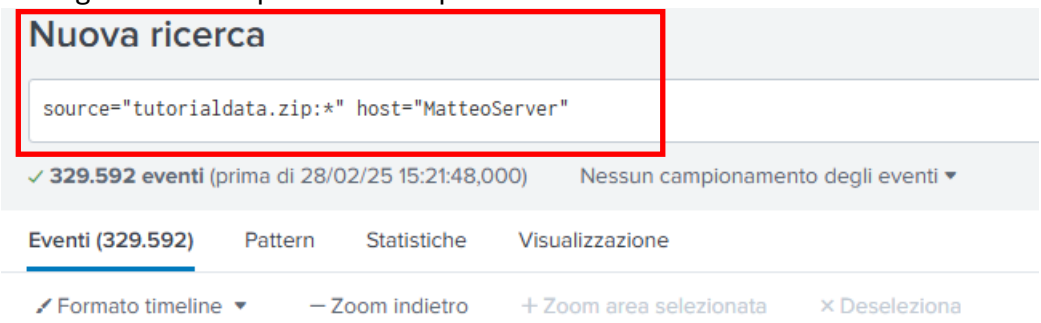
Immagine 14 – Visualizzazione eventi in Splunk



3.2 Query in Splunk, ricerche di Dati

Viene richiesto di creare e formulare delle query, nel linguaggio SPL, che ci permettano di trovare delle informazioni sensibili riguardo a possibili accessi non autorizzati al sistema; faremo utilizzo di tutte le parole chiave utili alle ricerche, dei campi ecc; è possibile comporre la query all'interno della sezione "Nuova ricerca"

Immagine 15 – Campo ricerca in Splunk



```
source="tutorialdata.zip:*" host="MatteoServer"
```

✓ **329.592 eventi** (prima di 28/02/25 15:21:48,000)

3.2.1. QUERY 1

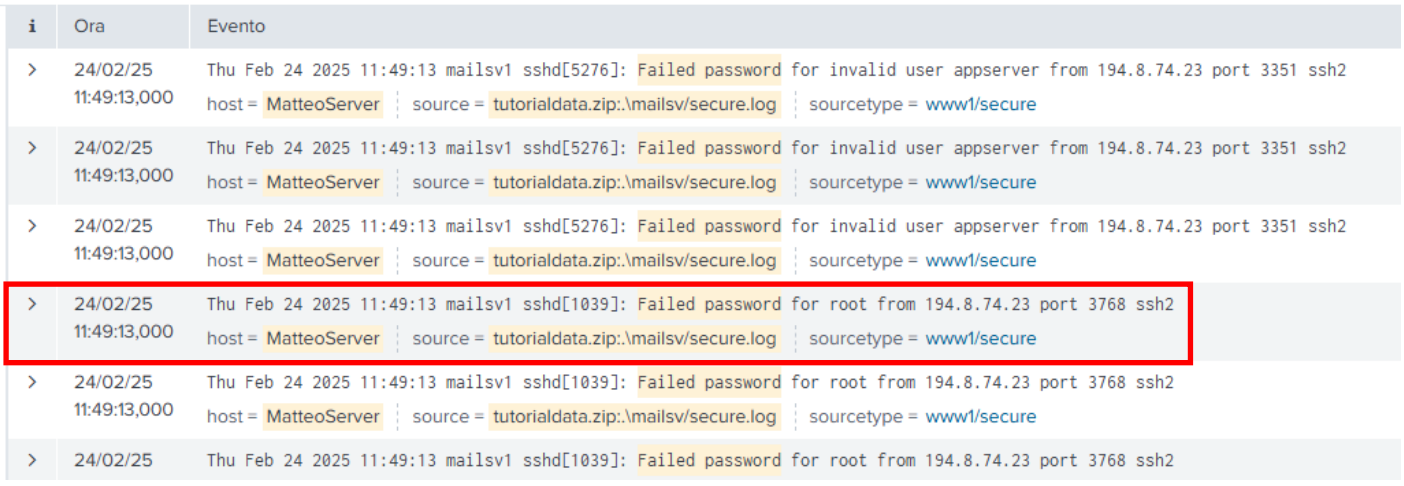
- Crea una query Splunk per identificare tutti i tentativi di accesso falliti "Failed password". La query dovrebbe mostrare il timestamp, l'indirizzo IP di origine, il nome utente e il motivo del fallimento.

Per ricercare quanto richiesto, utilizziamo la seguente query:

source="tutorialdata.zip:*" host="MatteoServer" "Failed password"

In questo modo, oltre ad indicare la source e l'host, chiediamo a Splunk di mostrarci solo gli eventi nei quali ci sono stati dei tentativi di accesso, ma non riusciti in quanto sono state inserite credenziali errate

Immagine 16 – eventi query 1



i	Ora	Evento
>	24/02/25 11:49:13,000	`Thu Feb 24 2025 11:49:13 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2` host = MatteoServer │ source = tutorialdata.zip:.\mailsv/secure.log │ sourcetype = www1/secure
>	24/02/25 11:49:13,000	`Thu Feb 24 2025 11:49:13 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2` host = MatteoServer │ source = tutorialdata.zip:.\mailsv/secure.log │ sourcetype = www1/secure
>	24/02/25 11:49:13,000	`Thu Feb 24 2025 11:49:13 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2` host = MatteoServer │ source = tutorialdata.zip:.\mailsv/secure.log │ sourcetype = www1/secure
>	24/02/25 11:49:13,000	`Thu Feb 24 2025 11:49:13 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2` host = MatteoServer │ source = tutorialdata.zip:.\mailsv/secure.log │ sourcetype = www1/secure
>	24/02/25 11:49:13,000	`Thu Feb 24 2025 11:49:13 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2` host = MatteoServer │ source = tutorialdata.zip:.\mailsv/secure.log │ sourcetype = www1/secure
>	24/02/25	`Thu Feb 24 2025 11:49:13 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2`

Analizzando in modo più approfondito l'evento nel riquadro rosso, otteniamo quanto segue e richiesto:

- **Timestamp:**
  - "Thu Feb 24 2025 11:49:13" indica la data e l'ora dell'evento.
  - "11:49:13,000" è il timestamp più preciso, con i millisecondi.
- **Indirizzo IP di origine:** 194.8.74.23
- **Nome utente:** root
- **Motivo del fallimento:** "Failed password" indica un tentativo di accesso fallito a causa di una password errata.

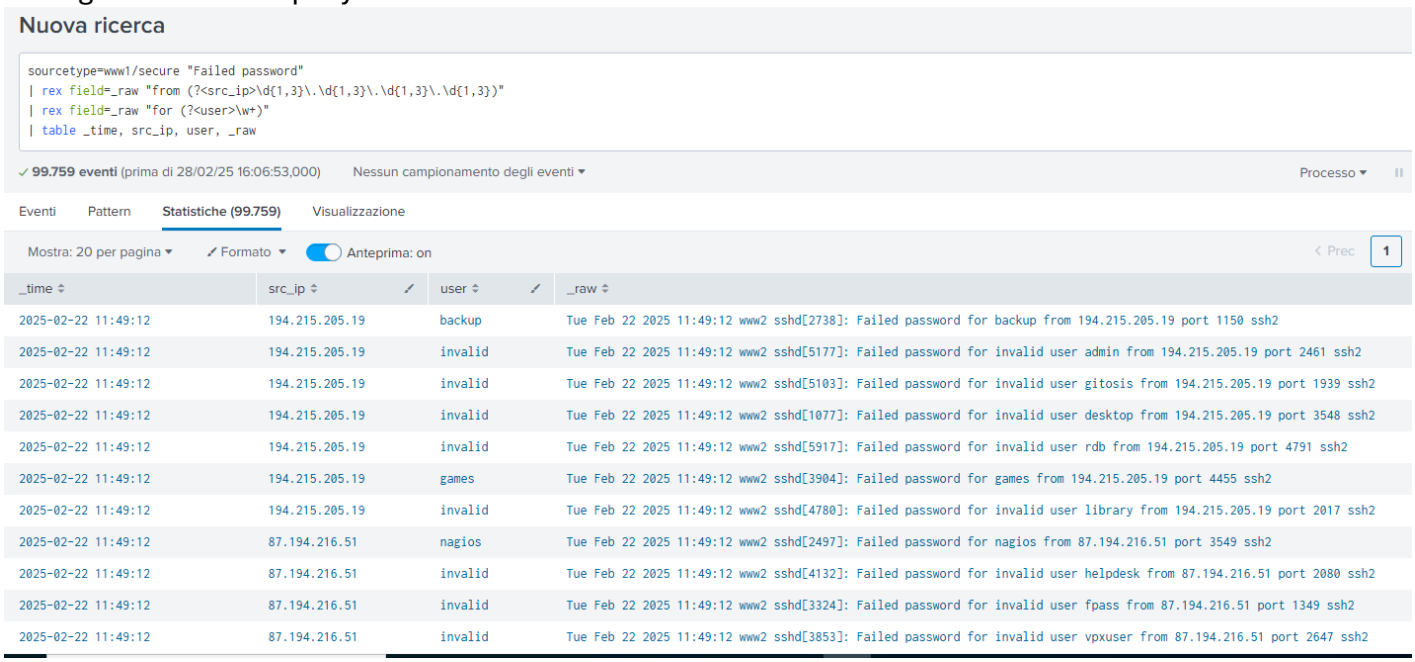
In sintesi, il messaggio riporta un tentativo di accesso fallito al server "MatteoServer" tramite SSH, proveniente dall'indirizzo IP 194.8.74.23, con il nome utente "root" e con una password errata.

Chiedendo aiuto all'AI, ho impostato la query in questo modo:

```
sourcetype=www1/secure "Failed password"
| rex field=_raw "from (?<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"
| rex field=_raw "for (?<user>\w+)"
| table _time, src_ip, user, _raw
```

Di seguito l'output della ricerca che Splunk ci propone

Immagine 17 – eventi query 1 con AI



Analisi della query:

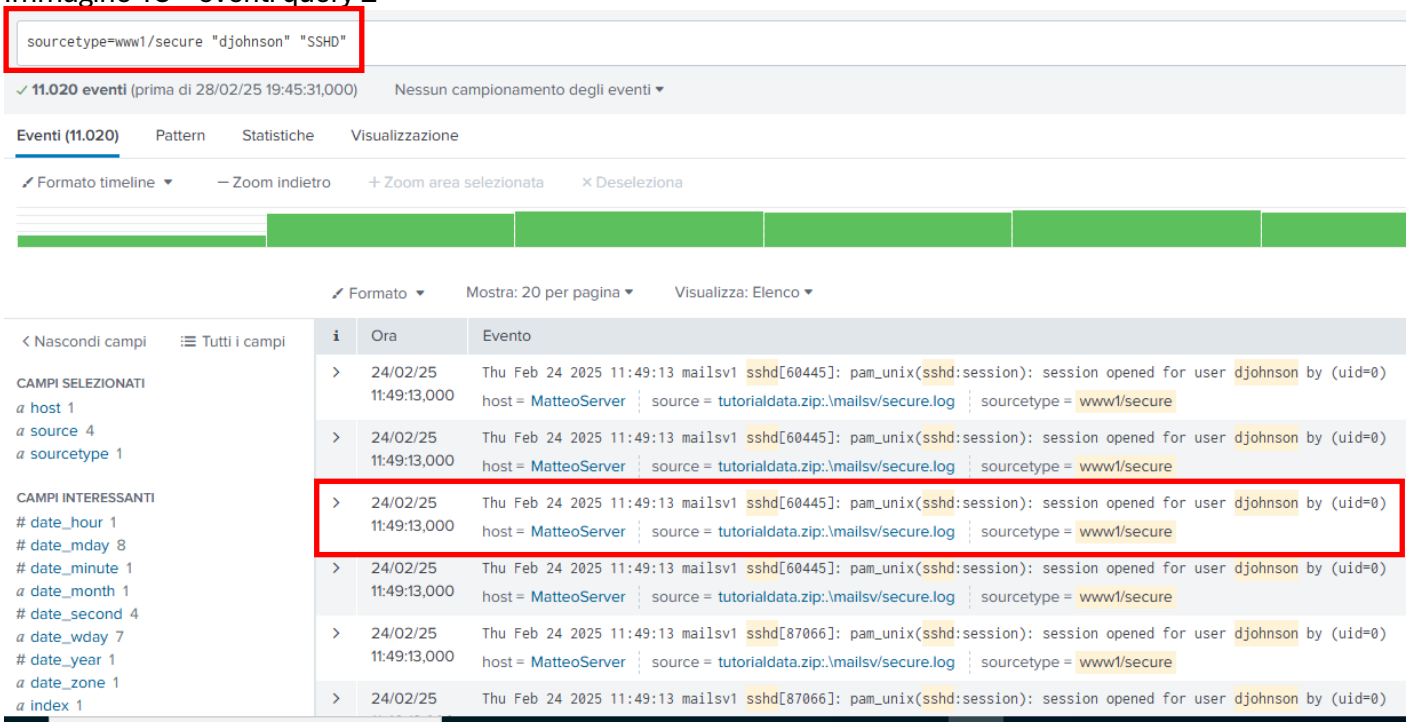
- **sourcetype=www1/secure "Failed password"**: Questa parte della query filtra gli eventi per selezionare solo quelli che provengono dalla sorgente "www1/secure" e contengono la frase "Failed password".
- **rex field=_raw "from (?<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"**: Questa espressione regolare estrae l'indirizzo IP di origine dal campo _raw e lo memorizza nel campo src_ip.
- **rex field=_raw "for (?<user>\w+)"**: Questa espressione regolare estrae il nome utente dal campo _raw e lo memorizza nel campo user.
- **table _time, src_ip, user, _raw**: Questa parte della query seleziona i campi da visualizzare nella tabella dei risultati: timestamp (_time), indirizzo IP di origine (src_ip), nome utente (user) e il messaggio di registro completo (_raw).

3.2.2 QUERY 2

- 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.

Per ricercare quanto richiesto, utilizziamo la seguente query:
sourcetype=www1/secure "djohnson" "SSHD"

Immagine 18 – eventi query 2



Analisi della query
sourcetype=www1/secure

- **sourcetype** identifica la fonte dei dati.
- **www1/secure** indica il tipo di log che Splunk sta cercando.

"djohnson"

- Cerca nei log tutti gli eventi che contengono il nome utente "djohnson".
- Questo aiuta a filtrare solo le attività di quell'utente, ignorando gli altri.

"SSHD"

- Cerca eventi che contengono la parola "SSHD".
- **SSHD (o sshd)** si riferisce al **servizio SSH daemon**, che gestisce le connessioni SSH in entrata.

Analizziamo per esempio, l'evento all'interno del riquadro rosso:
Informazioni estratte:

- **Utente:** "djohnson"
- **Timestamp:** "Thu Feb 24 2025 11:49:13" (Giovedì 24 febbraio 2025 alle 11:49:13)
- **ID utente (UID):** "uid=0"

Spiegazione:

- Il log mostra che l'utente "djohnson" ha aperto una sessione SSH.
- Il timestamp indica l'ora esatta in cui la sessione è stata aperta.
- "uid=0" Indica che la sessione è stata aperta dall'utente root. Anche se l'utente che ha aperto la sessione è "djohnson" è stato aperto con i privilegi di root, probabilmente usando il comando sudo.

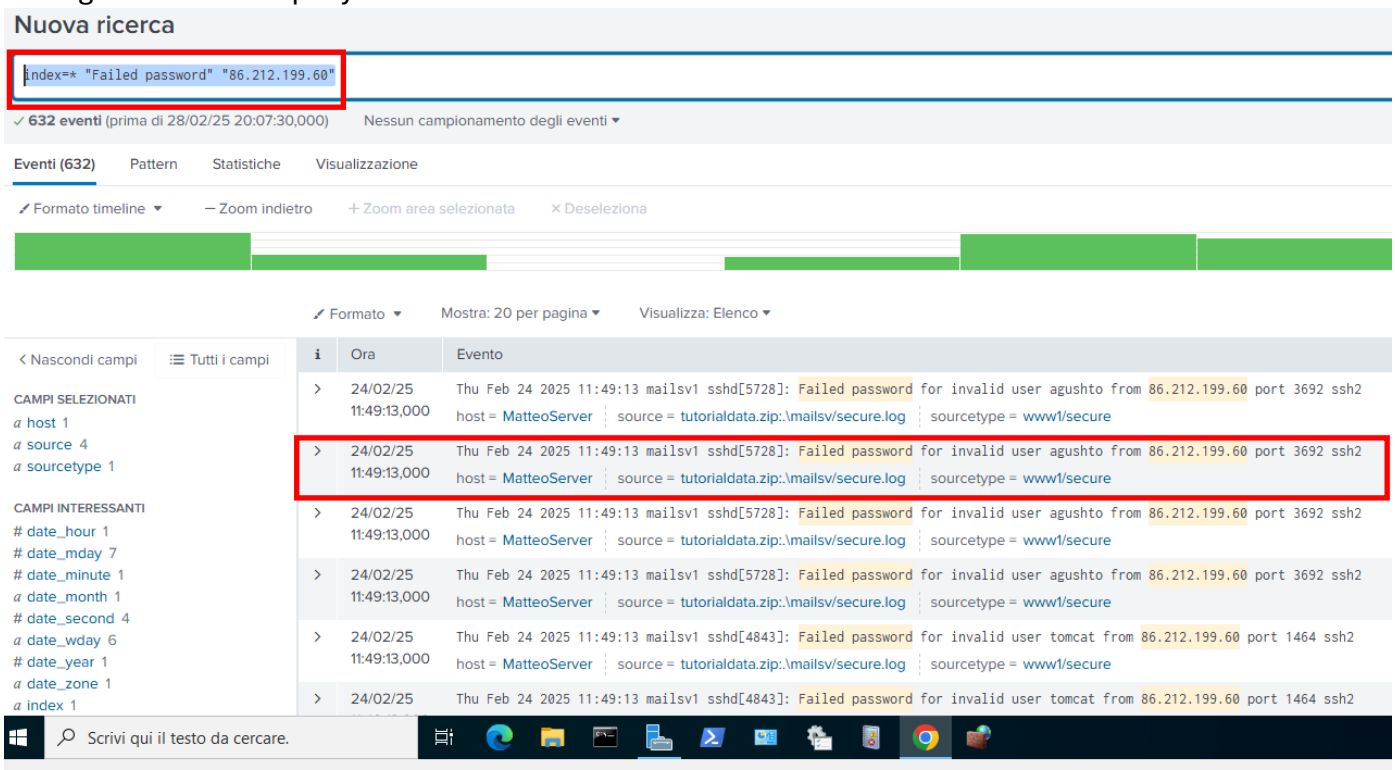
In sintesi:
si conferma che l'utente "djohnson" ha avviato una sessione SSH il 24 febbraio 2025 alle 11:49:13, e che questa sessione è stata avviata con i privilegi dell'utente root (uid=0).

3.2.3 QUERY 3

- 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.

Per ricercare quanto richiesto, utilizziamo la seguente query:
index=* "Failed password" "86.212.199.60"
Abbiamo filtrato in tutti gli eventi, per autenticazioni fallite e per l'indirizzo IP di provenienza

Immagine 19 – eventi query 3



Analisi della query:
index=*:

- Questo comando indica a Splunk di cercare in tutti gli indici disponibili. Gli indici in Splunk sono come database che contengono i tuoi dati di log. L'asterisco (*) è un carattere jolly che significa "tutti".

"Failed password":

- Questo è un termine di ricerca che filtra i risultati per includere solo gli eventi che contengono la frase esatta "Failed password". Questo è tipicamente usato per identificare i tentativi di accesso falliti.

"86.212.199.60":

- Questo è un altro termine di ricerca che filtra i risultati per includere solo gli eventi che contengono l'indirizzo IP "86.212.199.60". Questo è usato per identificare gli eventi provenienti da un indirizzo IP specifico.

In sintesi:
Questa query Splunk cerca in tutti gli indici di log per trovare tutti gli eventi che soddisfano entrambe le seguenti condizioni:

- L'evento contiene la frase "Failed password".

- L'evento contiene l'indirizzo IP "86.212.199.60".

In altre parole, questa query identifica tutti i tentativi di accesso falliti che provengono dall'indirizzo IP "86.212.199.60".

Analizziamo per esempio, l'evento all'interno del riquadro rosso:

Informazioni chiave estratte dal log:

- **Data e ora:** 24/02/25 Thu Feb 24 2025 11:49:13 (Giovedì 24 febbraio 2025 alle 11:49:13)
- **Host:** mailsv1
- **Processo:** sshd[5728] (il demone SSH con ID processo 5728)
- **Tipo di evento:** Failed password (password fallita)
- **Utente:** agushto (utente non valido)
- **Indirizzo IP di origine:** 86.212.199.60
- **Porta di origine:** 3692
- **Protocollo:** ssh2
- **Timestamp di fine evento:** 11:49:13,000
- **Host di origine:** MatteoServer
- **Fonte del log:** tutorialdata.zip:.\mailsv/secure.log
- **Tipo di origine:** www1/secure

Significato:

Questo log indica un tentativo di accesso SSH fallito. Un utente non valido, "agushto", ha cercato di accedere al server "mailsv1" dall'indirizzo IP 86.212.199.60 sulla porta 3692. Il tentativo è fallito a causa di una password errata.

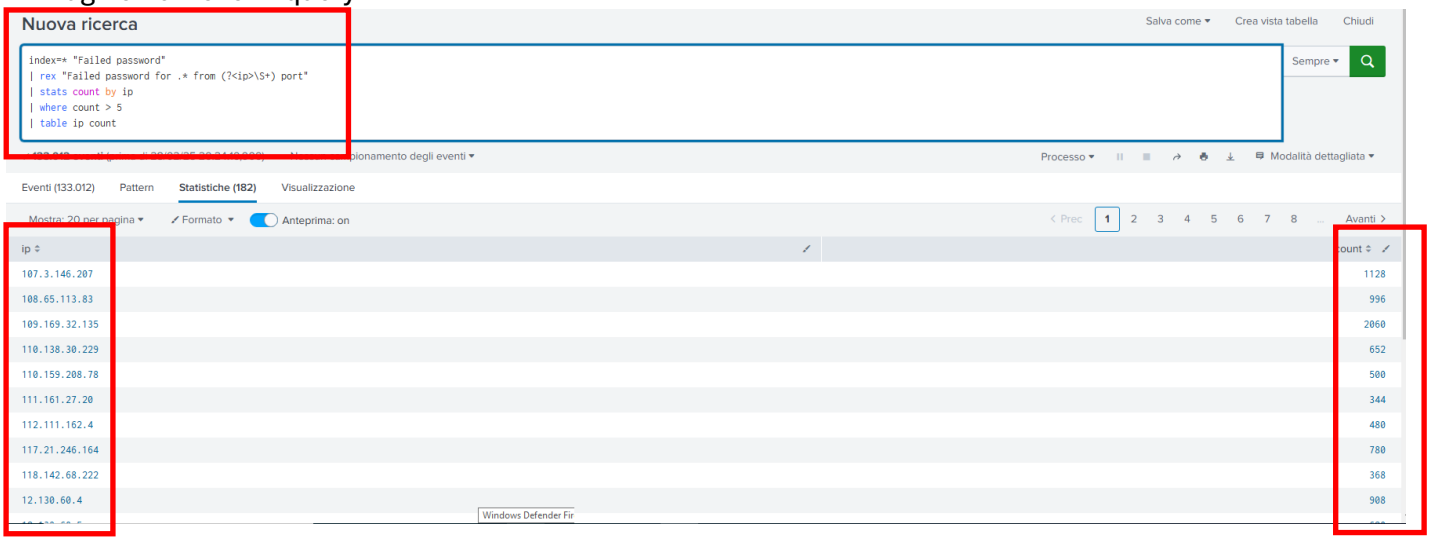
3.2.4 QUERY 4

➢ 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.

Per ricercare quanto richiesto, utilizziamo la seguente query:

```
index=* "Failed password"
| rex "Failed password for .* from (?<ip>\S+) port"
| stats count by ip
| where count > 5
| table ip count
```

Immagine 20 – eventi query 4



Da una nostra analisi, possiamo affermare che l'output a fornito due colonne principali: la prima mostrando tutti gli IP che per più di cinque volte hanno tentato l'accesso fornendo credenziali non corrette (Failed password) e la seconda colonna chiamata "Count" che mostra il numero effettivo di volte che hanno tentato l'accesso, comunque maggiore di 5 volte.

Analisi della query:
index=* "Failed password"

- **index=***: Indica a Splunk di cercare in tutti gli indici disponibili.
- **"Failed password"**: Filtra i risultati per includere solo gli eventi che contengono la frase esatta "Failed password", tipica dei log di autenticazione falliti.

| rex "Failed password for .* from (?<ip>\S+) port"

- **rex**: È un comando Splunk che usa le espressioni regolari per estrarre informazioni dai dati.
- **"Failed password for .* from (?<ip>\S+) port"**: Questa espressione regolare cerca la stringa "Failed password for", seguita da qualsiasi carattere (.) ripetuto zero o più volte (*), poi "from", uno spazio, e cattura una sequenza di caratteri non-spazio (\S+) in un campo chiamato "ip", infine uno spazio e la parola "port". In pratica, estrae l'indirizzo IP dalla stringa di log e lo assegna al campo "ip".

| stats count by ip

- **stats**: È un comando Splunk che calcola statistiche sui dati.
- **count by ip**: Conta il numero di eventi per ogni valore distinto del campo "ip" (l'indirizzo IP estratto).

| where count > 5

- **where**: Filtra i risultati in base a una condizione.
- **count > 5**: Mantiene solo i risultati in cui il conteggio degli eventi (tentativi di accesso falliti) per un indirizzo IP è maggiore di 5.

| table ip count

- **table**: Formatta l'output in una tabella.
- **ip count**: Specifica che la tabella deve includere le colonne "ip" (indirizzo IP) e "count" (numero di tentativi).

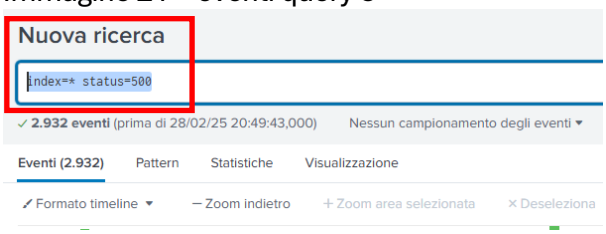
In sintesi:
Questa query estrae gli indirizzi IP dai log di accesso falliti, conta quanti tentativi sono stati fatti da ciascun indirizzo IP e mostra una tabella con gli indirizzi IP che hanno più di 5 tentativi falliti. È utile per identificare potenziali attacchi brute-force o attività sospette sulla rete.

3.2.5 QUERY 5

➢ Crea una query Splunk per trovare tutti gli Internal Server Error. Trarre delle conclusioni sui log analizzati utilizzando AI.

Per ricercare quanto richiesto, utilizziamo la seguente query:
index=* status=500
con questa query, filtriamo per tutti i log eventi (index=*) per lo status=500 che significa esattamente Internal Server Error

Immagine 21 – eventi query 5



i	Ora	Evento
>	24/02/25 18:18:59,000	`198.35.1.75 - - [24/Feb/2025:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&JSESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2324 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 645` host = MatteoServer ⁞ source = tutorialdata.zip:.\www1/access.log ⁞ sourcetype = access_combined_wcookie
>	24/02/25 18:18:59,000	`198.35.1.75 - - [24/Feb/2025:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&JSESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2324 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 645` host = MatteoServer ⁞ source = tutorialdata.zip:.\www1/access.log ⁞ sourcetype = access_combined_wcookie
>	24/02/25 18:18:59,000	`198.35.1.75 - - [24/Feb/2025:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&JSESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2324 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 645` host = MatteoServer ⁞ source = tutorialdata.zip:.\www1/access.log ⁞ sourcetype = access_combined_wcookie
>	24/02/25 18:18:59,000	`198.35.1.75 - - [24/Feb/2025:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&JSESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2324 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 645` host = MatteoServer ⁞ source = tutorialdata.zip:.\www1/access.log ⁞ sourcetype = access_combined_wcookie

Analisi della query:

index=*:

- Questo comando indica a Splunk di cercare in tutti gli indici disponibili. Come menzionato in precedenza, gli indici in Splunk sono come database che contengono i tuoi dati di log. L'asterisco (*) è un carattere jolly che significa "tutti".

status=500: (nel riquadro piccolo rosso)

- Questo è un termine di ricerca che filtra i risultati per includere solo gli eventi in cui il campo "status" è uguale a 500.
- Il codice di stato HTTP 500, "Internal Server Error", indica che il server ha incontrato una condizione imprevista che gli ha impedito di soddisfare la richiesta. In altre parole, si è verificato un errore sul server.

In sintesi:

Questa query Splunk cerca in tutti gli indici di log per trovare tutti gli eventi che soddisfano la seguente condizione:

- Il codice di stato HTTP è 500.

In pratica, questa query identifica tutti gli eventi di log che segnalano errori interni del server.

Analizziamo per esempio, l'evento all'interno del riquadro rosso:

Informazioni chiave estratte dal log:

- **Data e ora:** 24/02/25 18:18:59.000
- **Indirizzo IP client:** 138.35.1.75
- **Data e ora della richiesta:** [24/Feb/2025:18:18:59]
- **Metodo HTTP:** GET
- **URL richiesto:** /cart.do?action-addtocart&itemid=557&JSESSIONID=5018512FF4ADFF53099
- **Protocollo HTTP:** HTTP/1.1
- **Codice di stato HTTP:** 500 (Internal Server Error)
- **Dimensione della risposta:** 2324 byte
- **Referer:** http://www.buttercupgames.com/category.screen?categoryl
- **User agent:** Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.8.1884.40 Safari/536.5
- **Host:** MatteoServer
- **Origine del log:** tutorialdata.zip:www/access.log
- **Tipo di origine:** access_combined_wcookie

Interpretazione:

Questo log indica che un client con indirizzo IP 138.35.1.75 ha effettuato una richiesta GET all'URL /cart.do?action-addtocart&itemid=557&JSESSIONID=5018512FF4ADFF53099 sul server "MatteoServer". Il server ha risposto con un codice di stato HTTP 500, "Internal Server Error", indicando che si è verificato un errore sul server durante l'elaborazione della richiesta.