

# PROGETTO

**Analisi del Malware e Splunk  
M6W24-D4**

**28 / 02 / 2025**

**Cybersecurity Analyst**

Analisi del Malware e Splunk



**SOMMARIO**

Traccia Progetto	Pag. 2
Premessa e preparazione laboratorio	Pag. 2
Svolgimento del progetto	Pag. 5
Query in Splunk, ricerche di Dati	Pag. 11
Query 1	Pag. 12
Query 2	Pag. 14
Query 3	Pag. 15
Query 4	Pag. 16
Conclusione	Pag. 20

## 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

## 2. Premessa e preparazione laboratorio

### 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.

### 2.1 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:

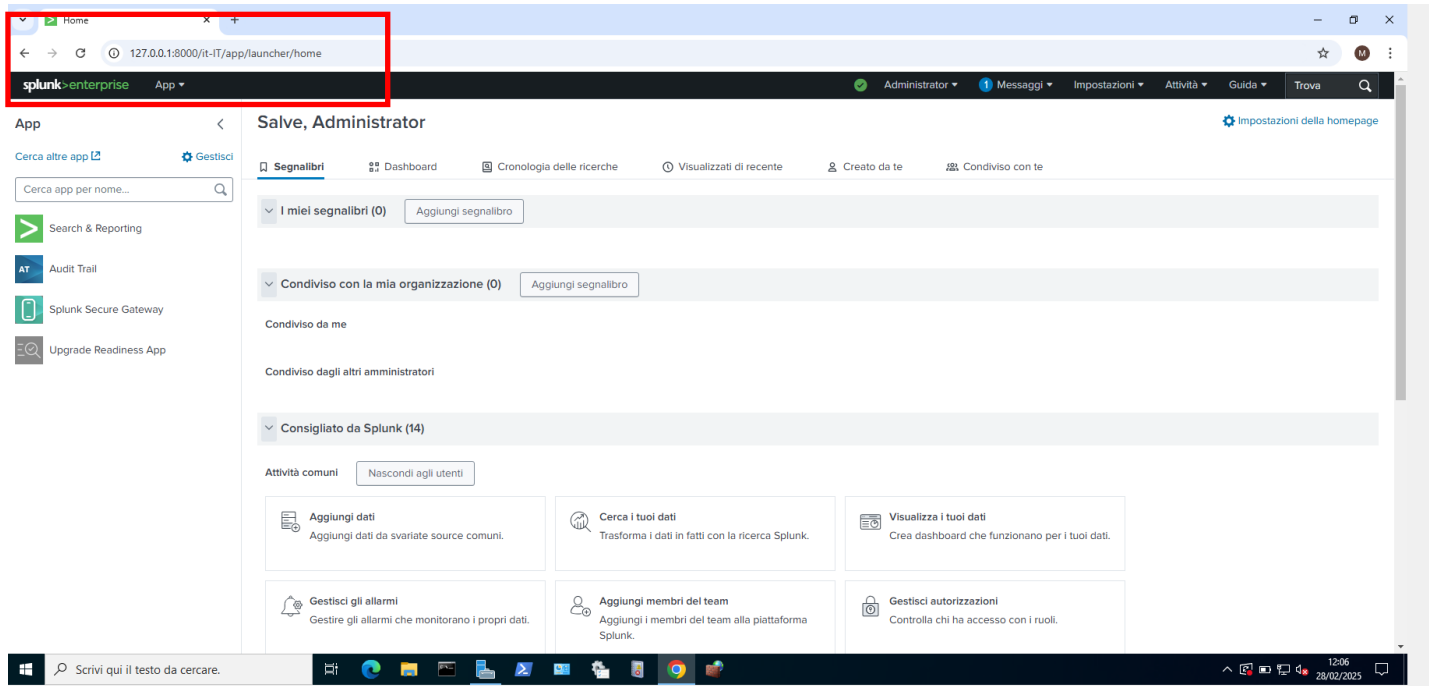
Il parsing è il processo di analisi dei dati grezzi per estrarre e strutturare le informazioni in campi definiti, come timestamp, indirizzi IP, URL, ecc. ○ Esempio: Estrazione di campi da un log di accesso Nginx come timestamp, metodo HTTP, URL richiesto, codice di stato.

### 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

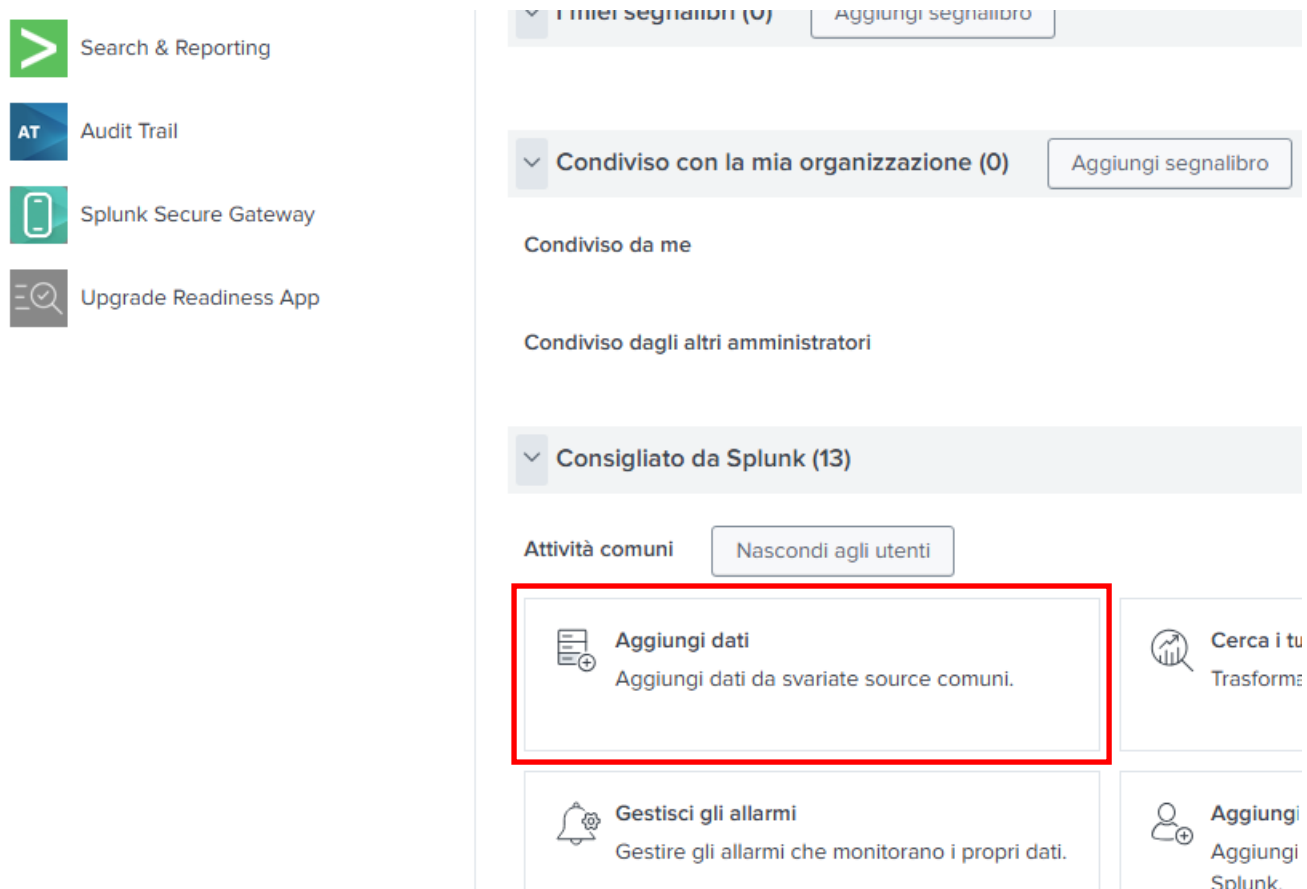




## 3 Svolgimento del Progetto


### 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”



Cliccare ora sulla sezione “carica”

Oppure, inserisci i dati utilizzando uno dei seguenti metodi



**Carica**  
file dal mio computer

File di log locali  
File strutturati locali (ad es. CSV)  
[Esercitazione per l'aggiunta di dati](#)



**Monitora**  
file e porte su questa istanza della piattaforma Splunk

File - HTTP - WMI - TCP/UDP - Script  
Input modulari per le fonti dati esterne



**Inoltra**  
dati da un forwarder di Splunk

File - TCP/UDP - Script

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

Aggiungi dati

Seleziona source

Scegliere un file da caricare nella piattaforma Splunk, cercando nel computer oppure trascinandolo nella casella di destinazione qui di seguito. [Ulteriori info](#)

File selezionato: Nessun file selezionato

Seleziona file

Trascina i file di dati qui

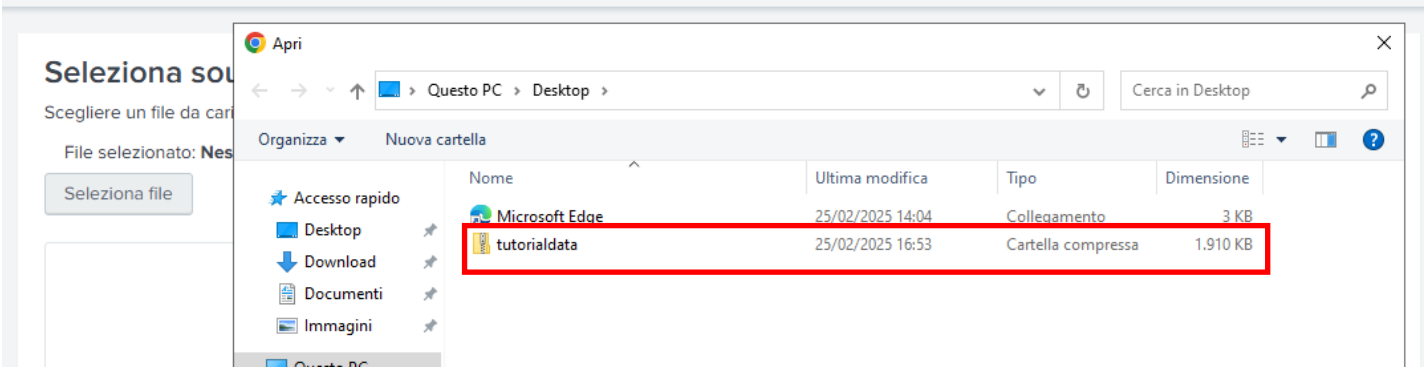
La dimensione di caricamento massima per i file è di 500 MB

**Domande frequenti**

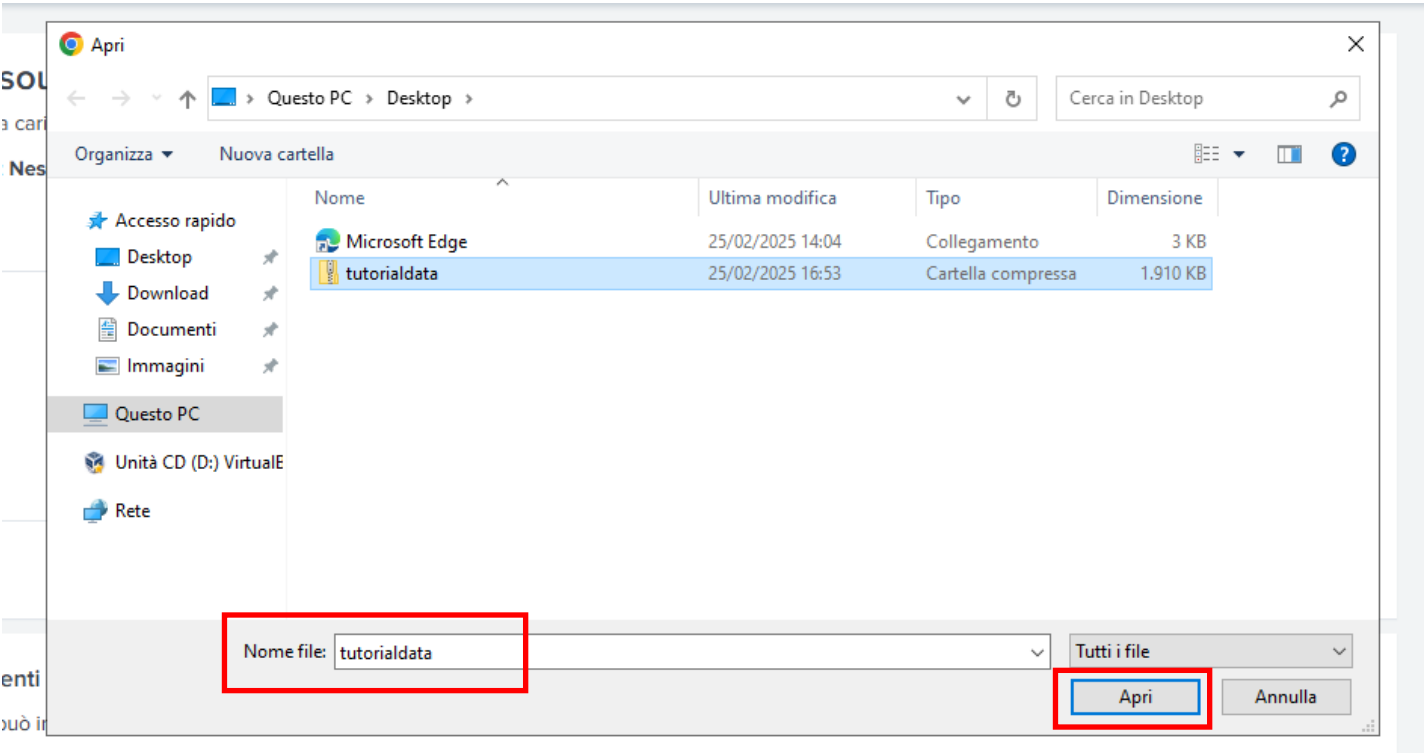
- > Quali tipi di file può indicizzare la piattaforma Splunk?
- > Che cos'è una fonte dati (source)?
- > Come faccio a inserire i dati remoti nella mia piattaforma Splunk?

Selezionare il file.zip da prendere in esame

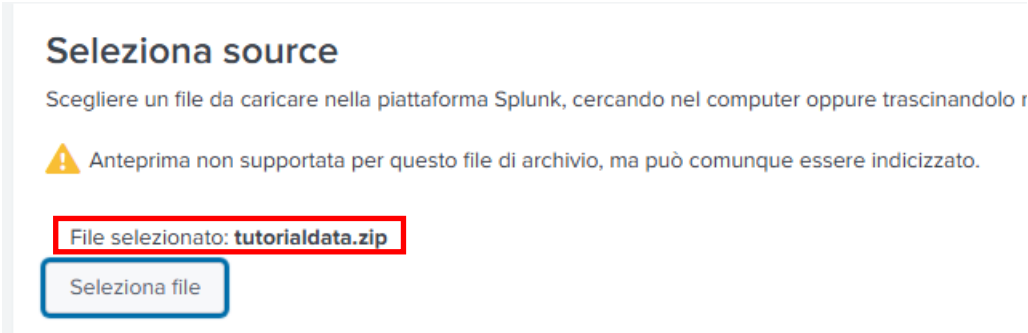




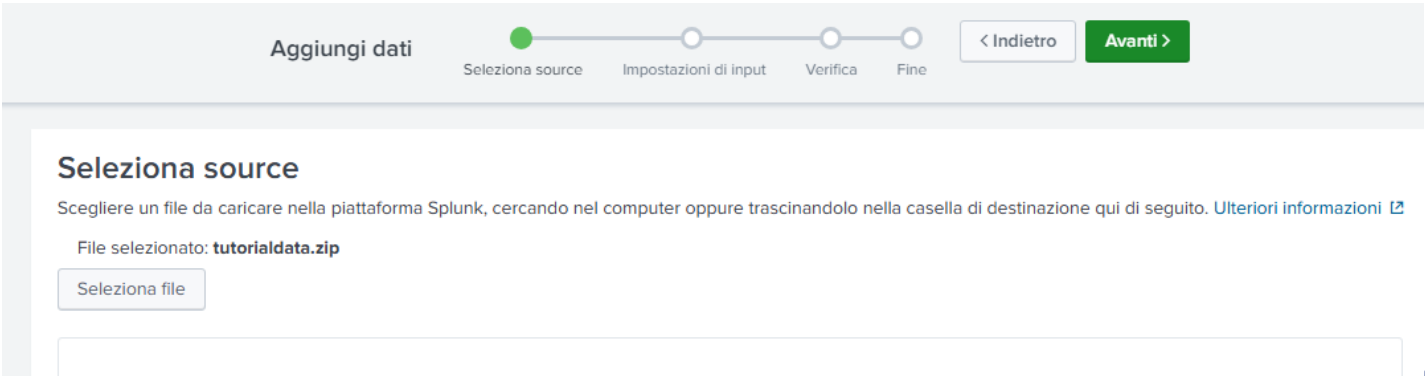
Cliccare su “Apri”



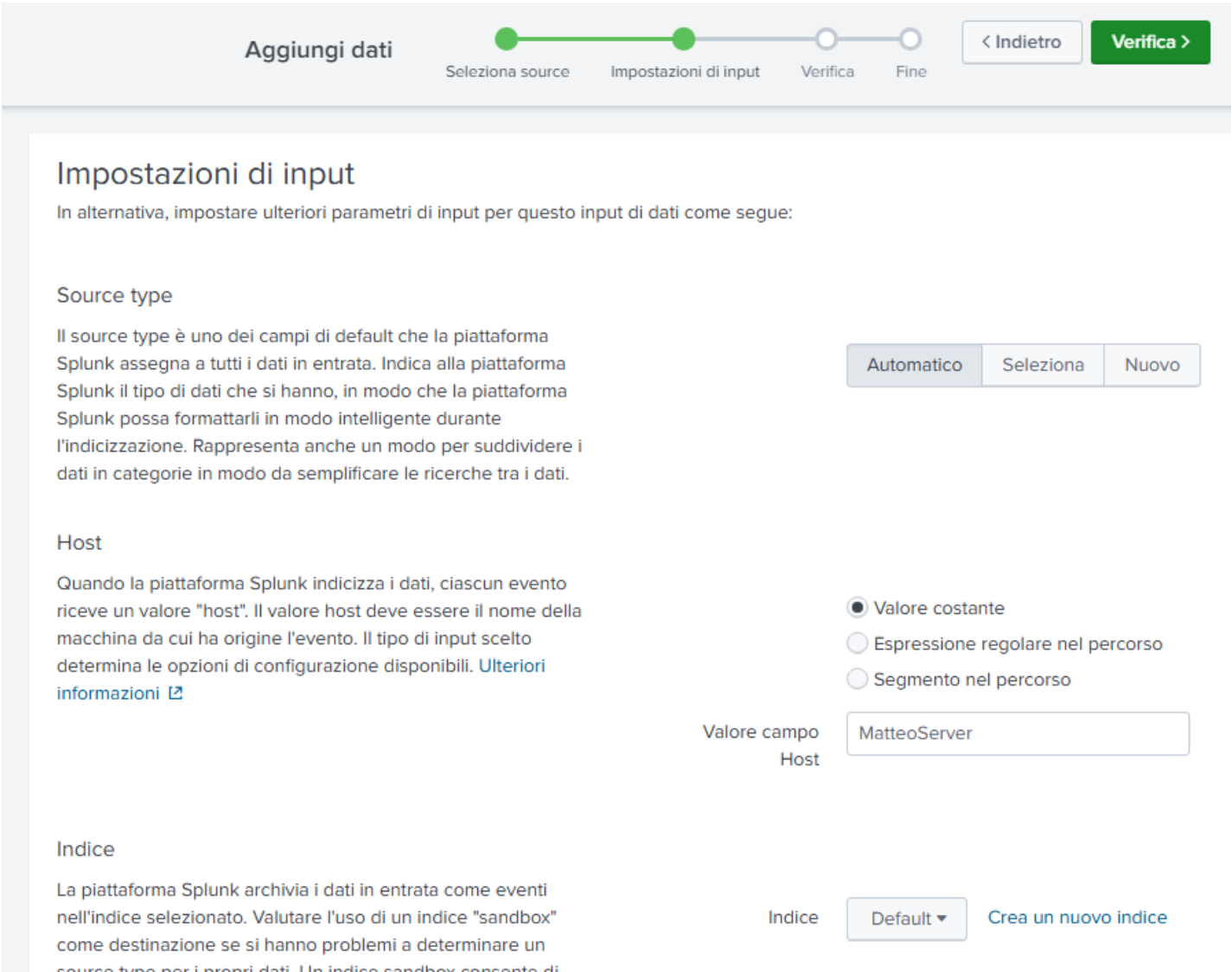
Una volta aperto il file, questa è la schermata che dobbiamo avere; il file è stato correttamente selezionato e aperto, quasi pronto per l’importazione



Cliccare ora su “Avanti”



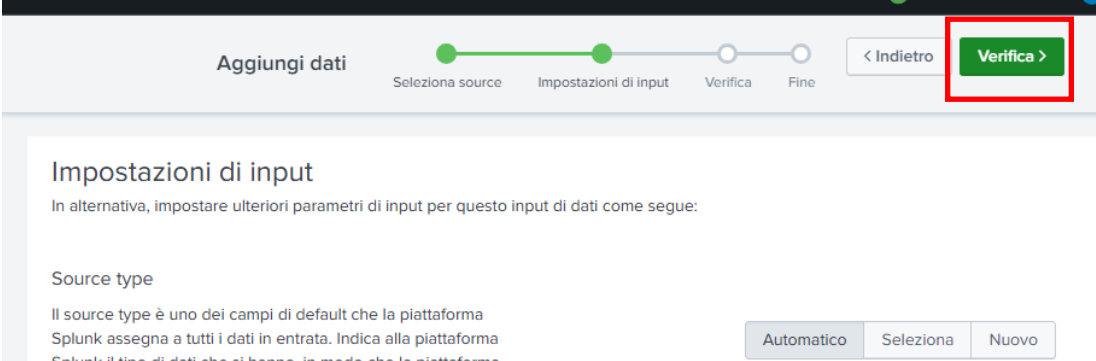
Una volta cliccato su avanti, Splunk ci mostrerà questa schermata:



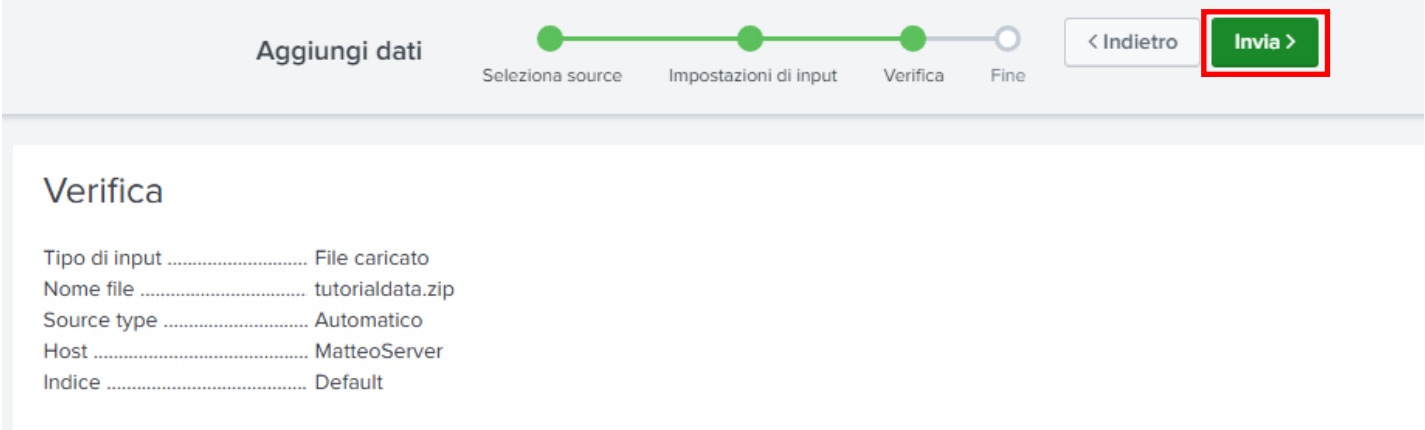
Splunk, per il suo corretto funzionamento e futura indicizzazione dei dati, si basa su settaggi molto importanti da effettuare prima di importare il file di dati analizzare, in quanto ogni file è a se e può avere origini differenti;

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”

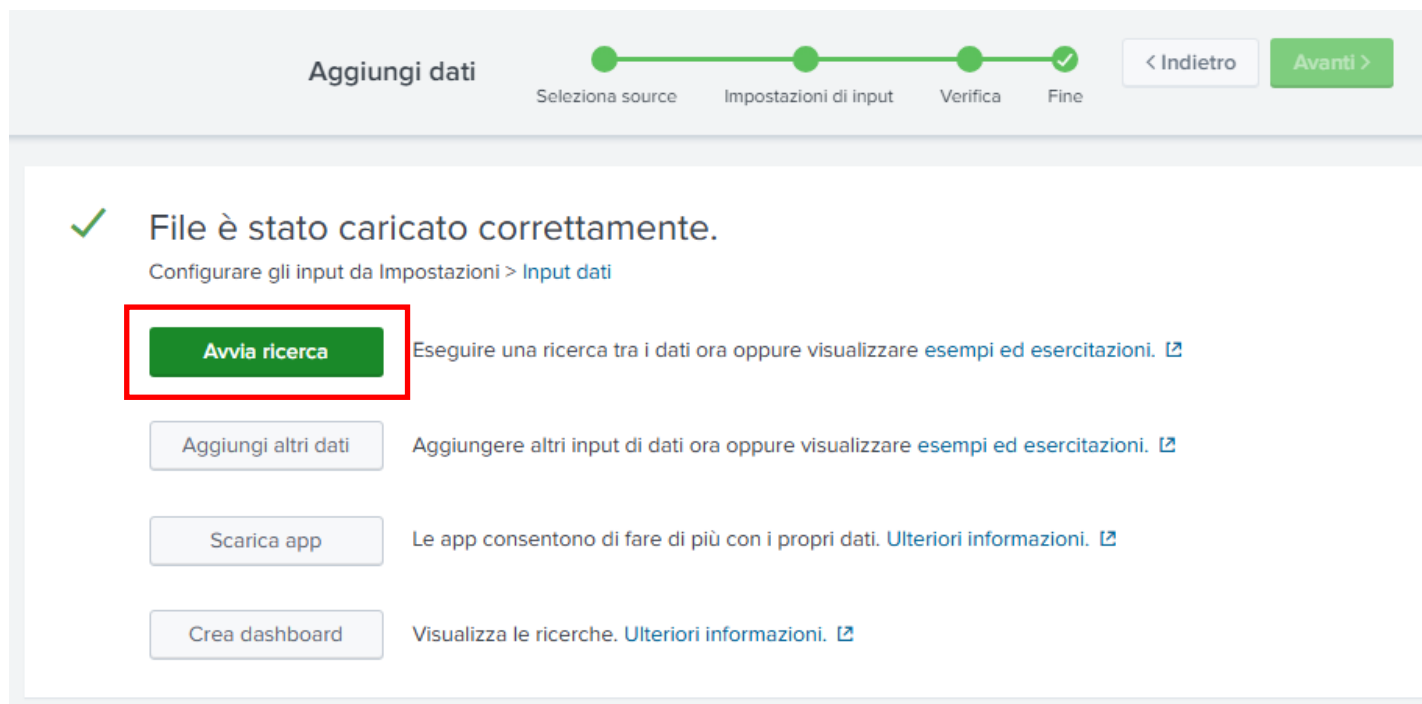


Dopo aver cliccato su “Verifica”, questa è la schermata che ci verrà proposta:



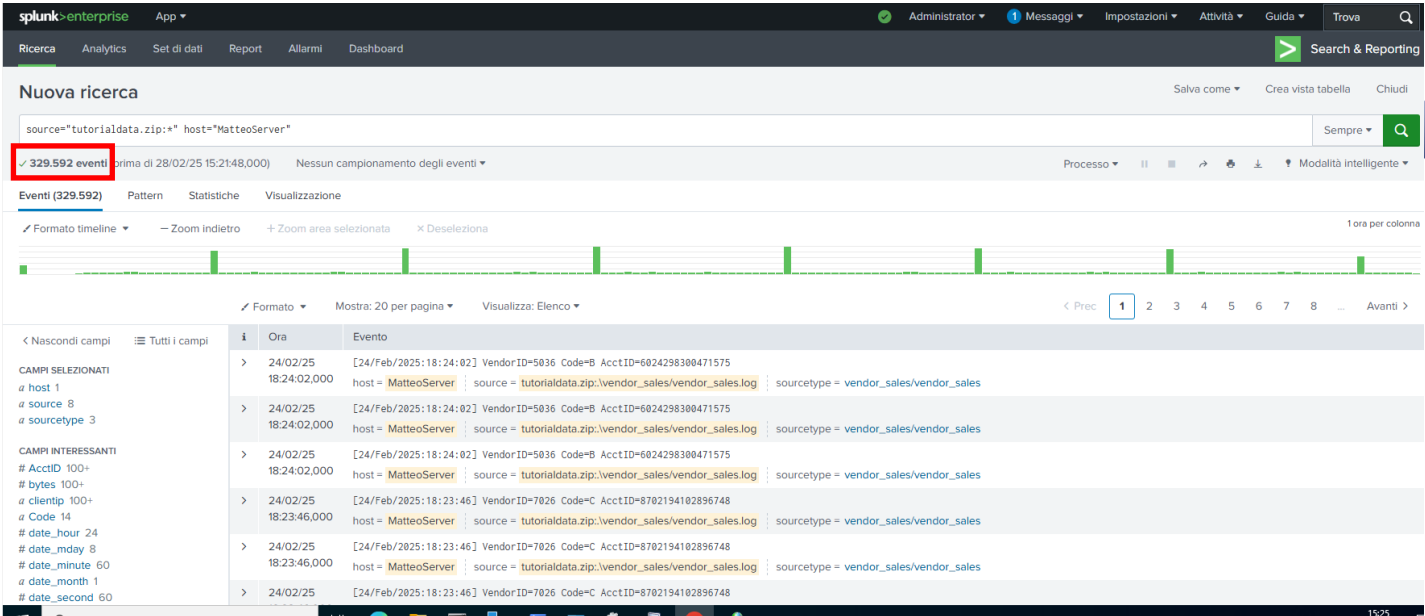
Cliccando su “Invia”, finalmente importiamo in Splunk il file dati “tutorialdata.zip” e il tool risulterà finalmente operativo.

A seguito di “Invia” di seguito la schermata che dobbiamo ottenere:

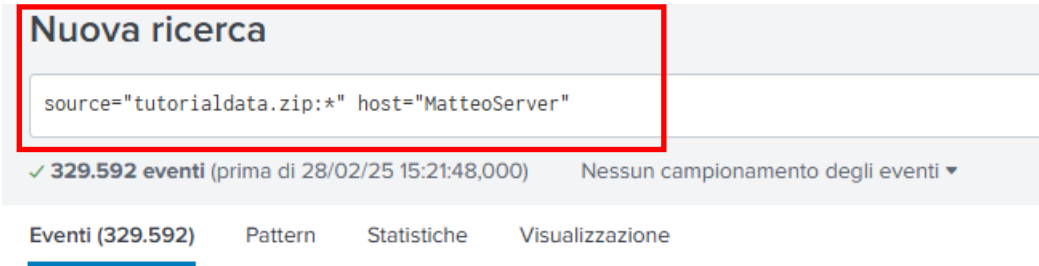


Procedere ora cliccando su “Avvia ricerca” per essere operativi al 100% e iniziare le ricerche di dati tramite apposite Query (SPL) di Splunk, per quanto richiesto in questo laboratorio.

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



**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”



**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

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

13

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

Nuova ricerca

```
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
```

✓ 99.759 eventi (prima di 28/02/25 16:06:53,000)    Nessun campionamento degli eventi

Processo

Eventi   Pattern   **Statistiche (99.759)**   Visualizzazione

Mostra: 20 per pagina

Formato

Anteprima: on

< Prec 1

_time	src_ip	user	_raw
2025-02-22 11:49:12	194.215.205.19	backup	Tue Feb 22 2025 11:49:12 www2 sshd[2738]: Failed password for backup from 194.215.205.19 port 1150 ssh2
2025-02-22 11:49:12	194.215.205.19	invalid	Tue Feb 22 2025 11:49:12 www2 sshd[5177]: Failed password for invalid user admin from 194.215.205.19 port 2461 ssh2
2025-02-22 11:49:12	194.215.205.19	invalid	Tue Feb 22 2025 11:49:12 www2 sshd[5103]: Failed password for invalid user gitosis from 194.215.205.19 port 1939 ssh2
2025-02-22 11:49:12	194.215.205.19	invalid	Tue Feb 22 2025 11:49:12 www2 sshd[1077]: Failed password for invalid user desktop from 194.215.205.19 port 3548 ssh2
2025-02-22 11:49:12	194.215.205.19	invalid	Tue Feb 22 2025 11:49:12 www2 sshd[5917]: Failed password for invalid user rdb from 194.215.205.19 port 4791 ssh2
2025-02-22 11:49:12	194.215.205.19	games	Tue Feb 22 2025 11:49:12 www2 sshd[3904]: Failed password for games from 194.215.205.19 port 4455 ssh2
2025-02-22 11:49:12	194.215.205.19	invalid	Tue Feb 22 2025 11:49:12 www2 sshd[4780]: Failed password for invalid user library from 194.215.205.19 port 2017 ssh2
2025-02-22 11:49:12	87.194.216.51	nagios	Tue Feb 22 2025 11:49:12 www2 sshd[2497]: Failed password for nagios from 87.194.216.51 port 3549 ssh2
2025-02-22 11:49:12	87.194.216.51	invalid	Tue Feb 22 2025 11:49:12 www2 sshd[4132]: Failed password for invalid user helpdesk from 87.194.216.51 port 2080 ssh2
2025-02-22 11:49:12	87.194.216.51	invalid	Tue Feb 22 2025 11:49:12 www2 sshd[3324]: Failed password for invalid user fpass from 87.194.216.51 port 1349 ssh2
2025-02-22 11:49:12	87.194.216.51	invalid	Tue Feb 22 2025 11:49:12 www2 sshd[3853]: Failed password for invalid user vpxuser from 87.194.216.51 port 2647 ssh2

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).

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"
```



15



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

**Nuova ricerca**

index=\* "Failed password" "86.212.199.60"

✓ 632 eventi (prima di 28/02/25 20:07:30,000) Nessun campionamento degli eventi ▼

Eventi (632) Pattern Statistiche Visualizzazione

Formato timeline Zoom indietro Zoom area selezionata Deseleziona

Formato Mostra: 20 per pagina Visualizza: Elenco

< Nascondi campi	Tutti i campi	i	Ora	Evento
CAMPI SELEZIONATI		>	24/02/25 11:49:13,000	Thu Feb 24 2025 11:49:13 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = MatteoServer source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
α host 1		>	24/02/25 11:49:13,000	Thu Feb 24 2025 11:49:13 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = MatteoServer source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
α source 4		>	24/02/25 11:49:13,000	Thu Feb 24 2025 11:49:13 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = MatteoServer source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
α sourcetype 1		>	24/02/25 11:49:13,000	Thu Feb 24 2025 11:49:13 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = MatteoServer source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
CAMPI INTERESSANTI		>	24/02/25 11:49:13,000	Thu Feb 24 2025 11:49:13 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = MatteoServer source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
# date_hour 1		>	24/02/25 11:49:13,000	Thu Feb 24 2025 11:49:13 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = MatteoServer source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
# date_mday 7		>	24/02/25 11:49:13,000	Thu Feb 24 2025 11:49:13 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = MatteoServer source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
# date_minute 1		>	24/02/25 11:49:13,000	Thu Feb 24 2025 11:49:13 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = MatteoServer source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
# date_month 1		>	24/02/25 11:49:13,000	Thu Feb 24 2025 11:49:13 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = MatteoServer source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
# date_second 4		>	24/02/25 11:49:13,000	Thu Feb 24 2025 11:49:13 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = MatteoServer source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
α date_wday 6		>	24/02/25 11:49:13,000	Thu Feb 24 2025 11:49:13 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = MatteoServer source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
# date_year 1		>	24/02/25 11:49:13,000	Thu Feb 24 2025 11:49:13 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = MatteoServer source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
α date_zone 1		>	24/02/25 11:49:13,000	Thu Feb 24 2025 11:49:13 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = MatteoServer source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
α index 1		>	24/02/25 11:49:13,000	Thu Feb 24 2025 11:49:13 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = MatteoServer source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure

Scrive qui il testo da cercare.

## 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.

### 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
```

ip	count
107.3.146.207	1128
108.65.113.83	996
109.169.32.135	2060
110.138.30.229	652
110.159.208.78	500
111.161.27.20	344
112.111.162.4	480
117.21.246.164	780
118.142.68.222	368
12.130.60.4	908

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.

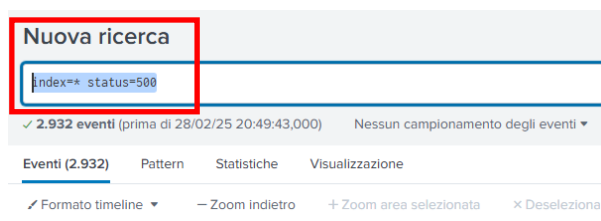
## QUERY 5

- 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



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?categoryI d=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:www/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?categoryI d=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:www/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?categoryI d=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:www/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?categoryI d=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:www/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?categoryI>
- 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.

### Conclusioni sull'analisi dei log in Splunk:

L'analisi dei log utilizzando Splunk ha permesso di identificare diversi eventi rilevanti riguardanti la sicurezza e l'affidabilità del sistema. In particolare, le query create hanno fornito informazioni dettagliate sui tentativi di accesso falliti e riusciti, nonché sugli errori del server che potrebbero indicare problematiche più gravi.

1. **Tentativi di accesso falliti ("Failed password"):** La query ha evidenziato i tentativi di accesso non riusciti, aiutando a monitorare eventuali attività sospette, come attacchi di forza bruta. La raccolta del timestamp, dell'indirizzo IP di origine, del nome utente e del motivo del fallimento è stata fondamentale per comprendere la natura e la provenienza di tali tentativi.
2. **Sessioni SSH riuscite:** La query specifica per l'utente "djohnson" ha permesso di monitorare e verificare le sessioni SSH legittime, garantendo che le operazioni effettuate fossero autorizzate e tracciabili.
3. **Tentativi di accesso falliti provenienti da un IP specifico:** Identificare i tentativi falliti provenienti dall'indirizzo IP "86.212.199.60" ha permesso di individuare in modo mirato eventuali rischi associati a quel particolare IP, utile per azioni correttive come il blocco di indirizzi sospetti.
4. **Indirizzi IP con più di 5 tentativi di accesso falliti:** Questa query ha aiutato a individuare potenziali fonti di attacco automatizzato, evidenziando gli indirizzi IP che potrebbero essere coinvolti in attività di brute-force. Monitorare questi indirizzi consente di prevenire accessi non autorizzati e attivare misure di sicurezza, come il blocco temporaneo degli IP in questione.
5. **Internal Server Errors:** Identificare gli errori del server interno (500) è stato cruciale per diagnosticare problemi tecnici e di performance del sistema. Questi errori potrebbero indicare malfunzionamenti o configurazioni errate, necessitando una revisione approfondita per prevenire il deterioramento delle performance del sistema.

In generale, l'uso di Splunk ha consentito di estrarre informazioni vitali per la sicurezza e la gestione del sistema, permettendo di intervenire tempestivamente per ridurre i rischi associati agli attacchi informatici e migliorare l'affidabilità del sistema. Inoltre, l'uso dell'intelligenza artificiale ha contribuito ad analizzare i pattern emergenti dai dati, migliorando la nostra capacità di identificare anomalie e rispondere a incidenti in tempo reale.