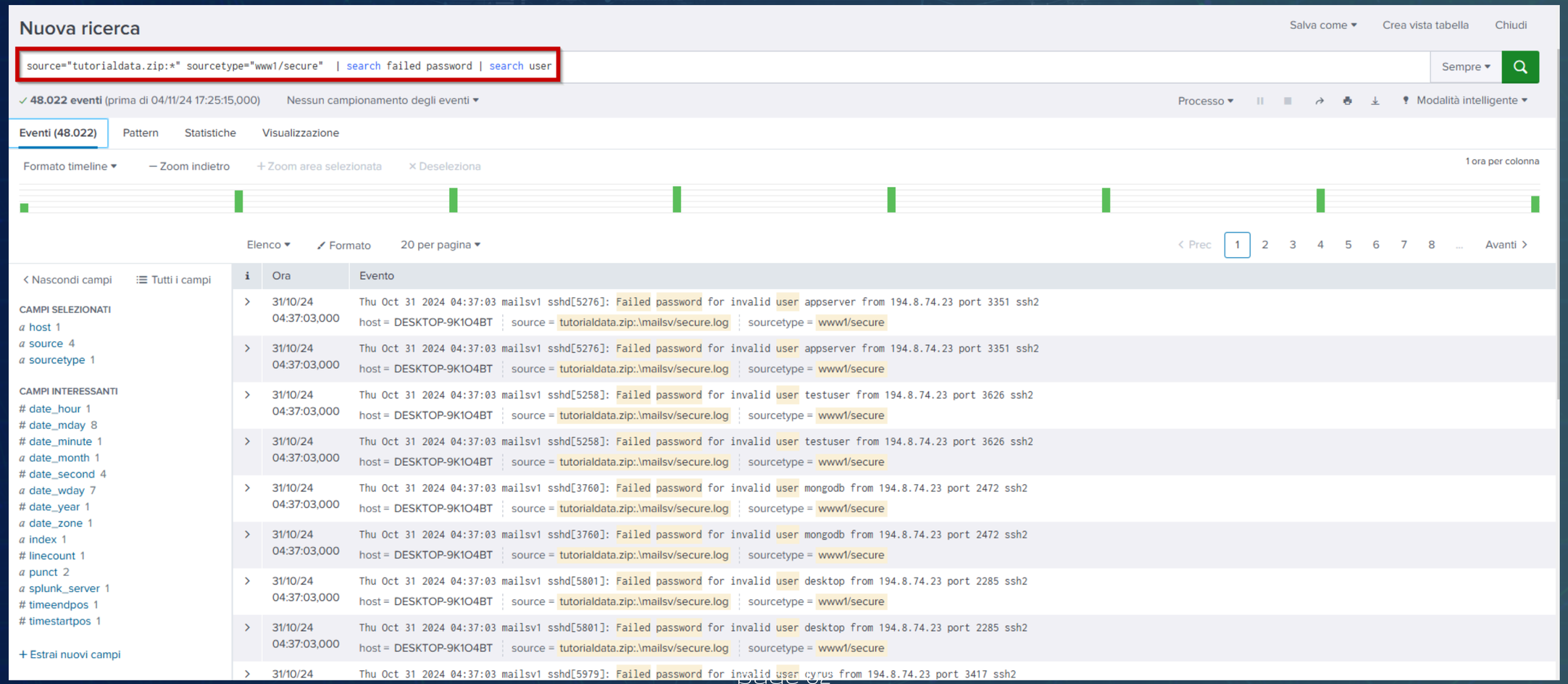
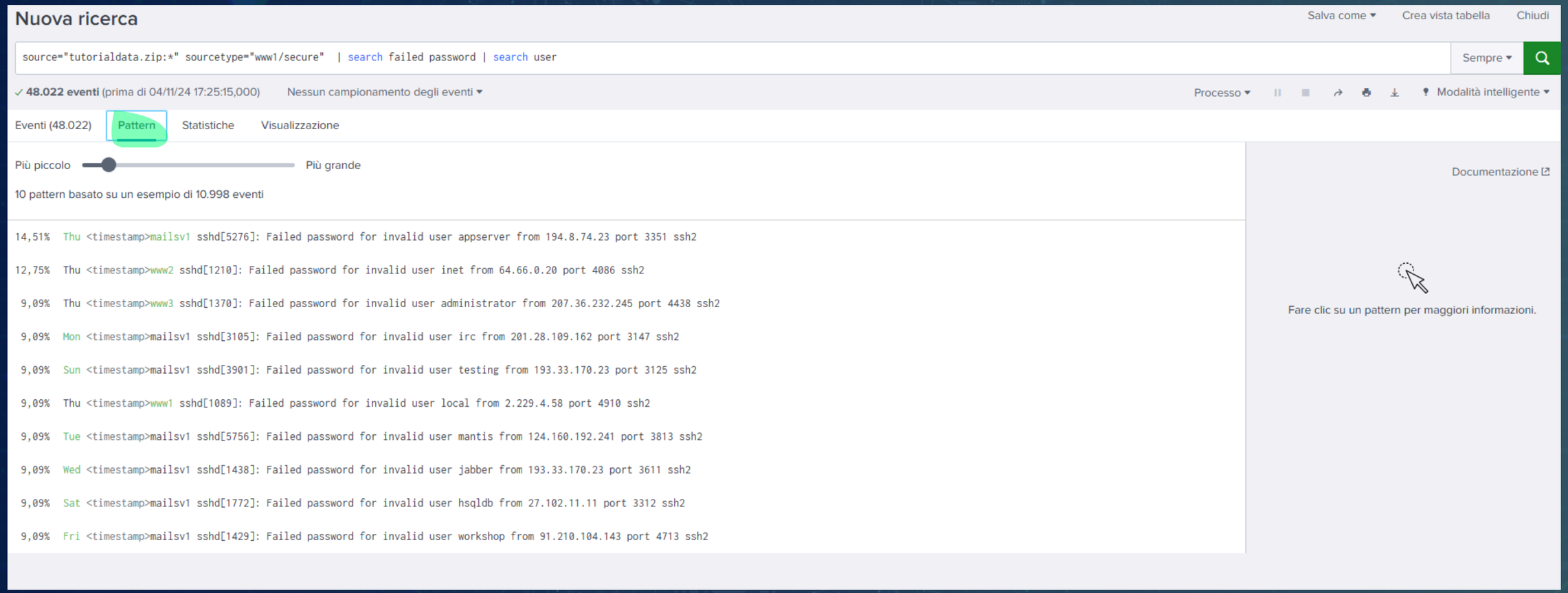
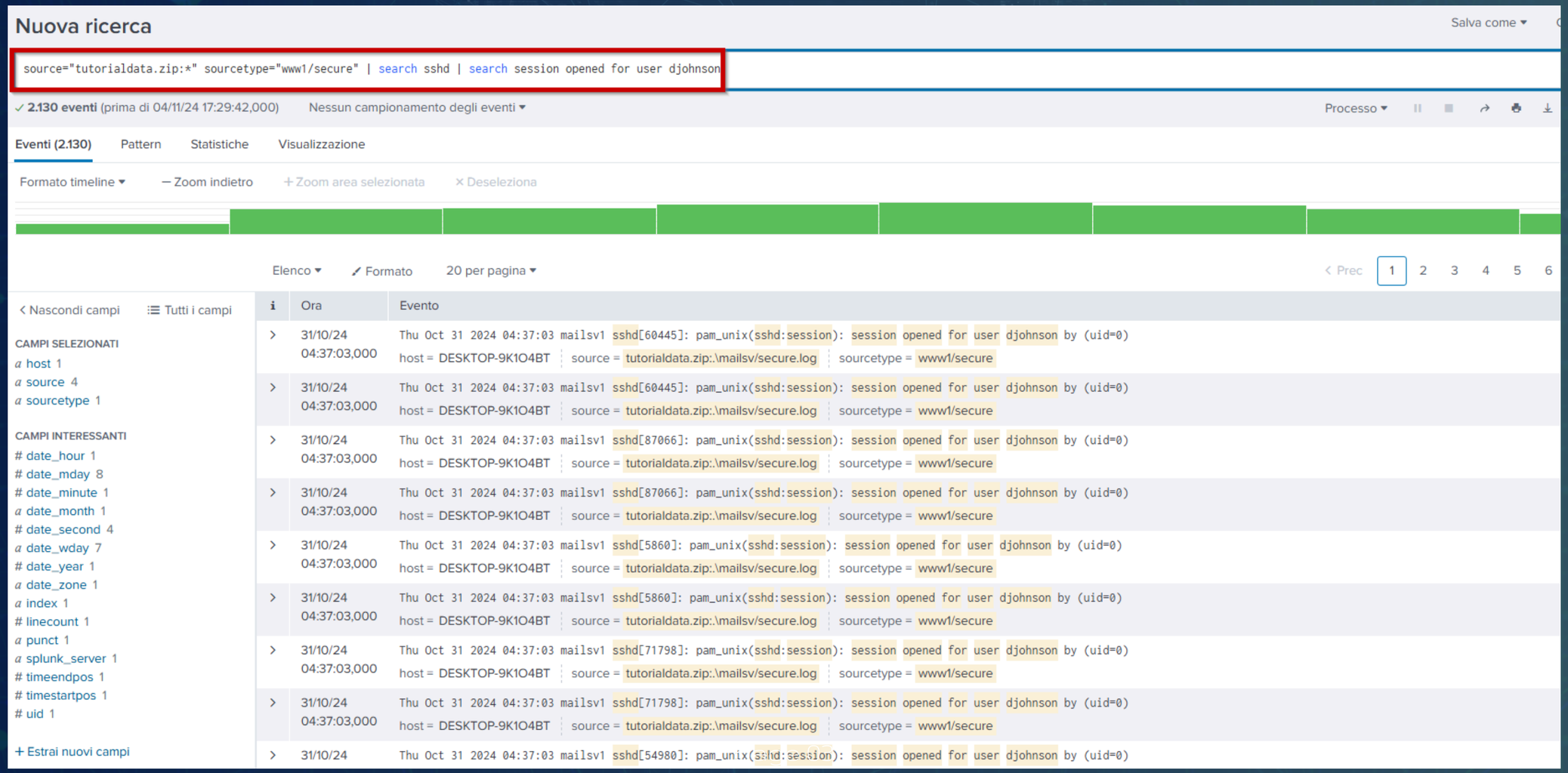
THE PROGECT

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.




Nuova ricerca
Salva come
Crea vista tabella
Chiudi
source="tutorialdata.zip:*" sourcetype="www1/secure" | search failed password | search user
Sempre
48.022 eventi (prima di 04/11/24 17:25:15,000)
Nessun campionamento degli eventi
Processo
Modalità intelligente
Eventi (48.022)
Pattern
Statistiche
Visualizzazione
Più piccolo
Più grande
10 pattern basato su un esempio di 10.998 eventi
Documentazione
14,51% Thu <timestamp>mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2
12,75% Thu <timestamp>www2 sshd[1210]: Failed password for invalid user inet from 64.66.0.20 port 4086 ssh2
9,09% Thu <timestamp>www3 sshd[1370]: Failed password for invalid user administrator from 207.36.232.245 port 4438 ssh2
9,09% Mon <timestamp>mailsv1 sshd[3105]: Failed password for invalid user irc from 201.28.109.162 port 3147 ssh2
9,09% Sun <timestamp>mailsv1 sshd[3901]: Failed password for invalid user testing from 193.33.170.23 port 3125 ssh2
9,09% Thu <timestamp>www1 sshd[1089]: Failed password for invalid user local from 2.229.4.58 port 4910 ssh2
9,09% Tue <timestamp>mailsv1 sshd[5756]: Failed password for invalid user mantis from 124.160.192.241 port 3813 ssh2
9,09% Wed <timestamp>mailsv1 sshd[1438]: Failed password for invalid user jabber from 193.33.170.23 port 3611 ssh2
9,09% Sat <timestamp>mailsv1 sshd[1772]: Failed password for invalid user hsqldb from 27.102.11.11 port 3312 ssh2
9,09% Fri <timestamp>mailsv1 sshd[1429]: Failed password for invalid user workshop from 91.210.104.143 port 4713 ssh2
Fare clic su un pattern per maggiori informazioni.

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.



Nuova ricerca

Salva come ▾ Crea vista tabella Chiudi

```
source="tutorialdata.zip:*" sourcetype="www1/secure" | search sshd | search session opened for user djohnson
```

Sempre ▾

✓ **2.130 eventi** (prima di 04/11/24 17:29:42,000) Nessun campionamento degli eventi ▾

Processo ▾ Modalità intelligente ▾

Eventi (2.130) Pattern Statistiche Visualizzazione

Più piccolo Più grande

1 pattern basato su un esempio di 2.130 eventi

⚠ Un numero di eventi inferiore a 5.000 potrebbe generare pattern di bassa qualità. Provare a effettuare una ricerca in un intervallo temporale più ampio o con meno vincoli.

100% Thu <timestamp>mailsv1 sshd[60445]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)

EVENTI STIMATI

2,13 migliaio/a

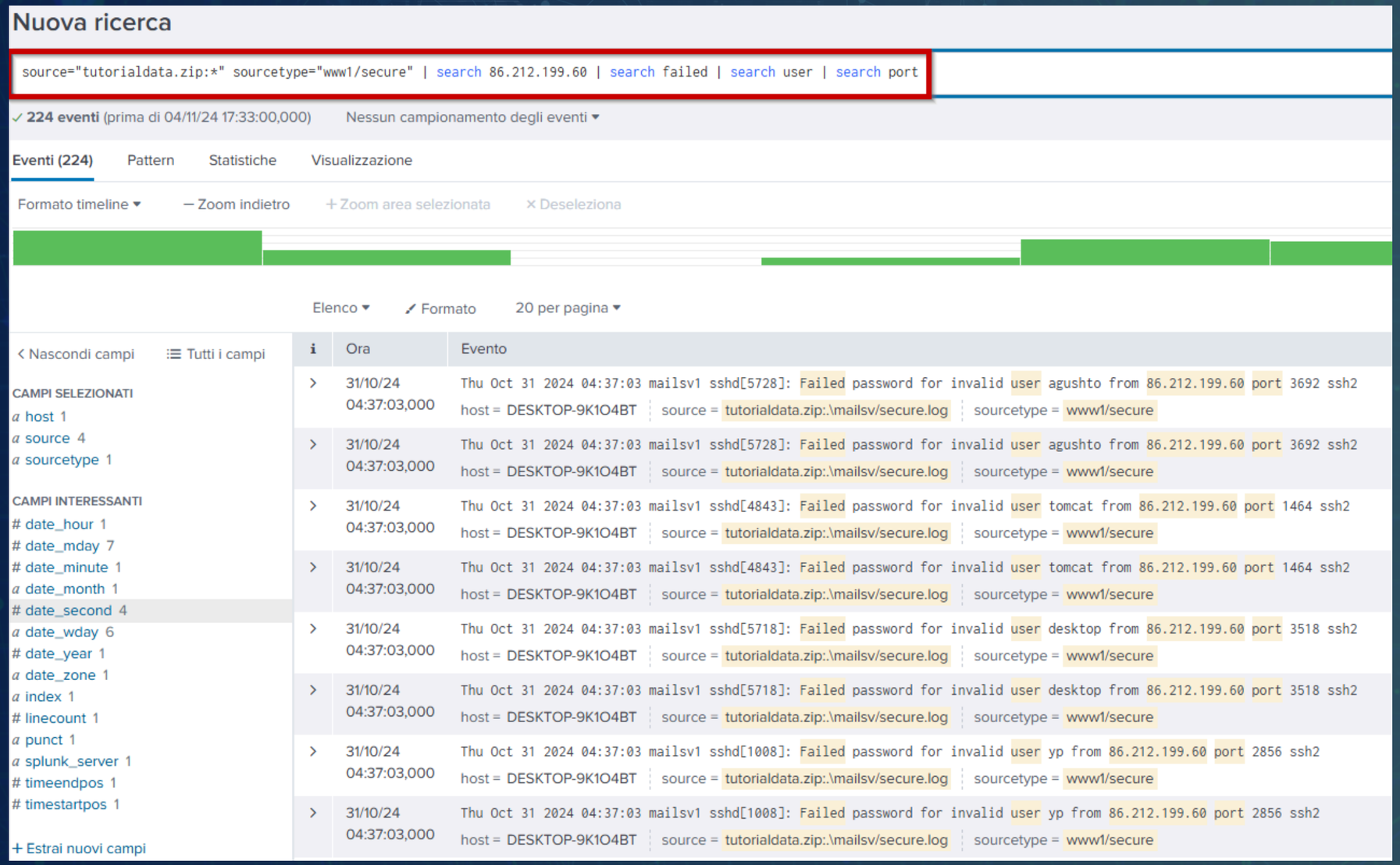
Visualizza eventi

RICERCA

(source="tutorialdata.zip:*" sourcetype="www1/secure" djohnson for opened session sshd user)

Salva come event type Crea allarme

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.



Nuova ricerca

```
source="tutorialdata.zip:*" sourcetype="www1/secure" | search 86.212.199.60 | search failed | search user | search port
```

✓ **224 eventi** (prima di 04/11/24 17:33:00,000) Nessun campionamento degli eventi ▾ Processo

Eventi (224) Pattern Statistiche Visualizzazione

Più piccolo Più grande

6 pattern basato su un esempio di 224 eventi

⚠ Un numero di eventi inferiore a 5.000 potrebbe generare pattern di bassa qualità. Provare a effettuare una ricerca in un intervallo temporale più ampio o con meno vincoli.

```
27,68%  Thu <timestamp>mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2

18,75%  Mon <timestamp>mailsv1 sshd[1399]: Failed password for invalid user administrator from 86.212.199.60 port 3447 ssh2

11,61%  Tue <timestamp>www3 sshd[3883]: Failed password for invalid user noone from 86.212.199.60 port 1583 ssh2

 6,25%  Wed <timestamp>www3 sshd[3129]: Failed password for invalid user services from 86.212.199.60 port 1393 ssh2

 7,14%  Thu <timestamp>www2 sshd[3218]: Failed password for invalid user hsqldb from 86.212.199.60 port 4379 ssh2

 5,36%  Sun <timestamp>www3 sshd[1214]: Failed password for invalid user email from 86.212.199.60 port 4130 ssh2
```

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.

Nuova ricerca

Salva come | Crea vista tabella | Chiudi

```
source="tutorialdata.zip:*" sourcetype="www1/secure" | rex "Failed password for .* from (?<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"
| stats count as num_attempts by src_ip
| where num_attempts > 5
| table src_ip num_attempts
| rename src_ip as "IP di Origine", num_attempts as "Numero di Tentativi"
```

Sempre

✓ **80.176 eventi** (prima di 04/11/24 17:37:37,000) Nessun campionamento degli eventi

Processo | Modalità intelligente

Eventi | Pattern | **Statistiche (182)** | Visualizzazione

20 per pagina | Formato | Anteprima

< Prec 1 2 3 4 5 6 7 8 ... Avanti >

IP di Origine	Numero di Tentativi
107.3.146.207	564
108.65.113.83	498
109.169.32.135	1030
110.138.30.229	326
110.159.208.78	250
111.161.27.20	172
112.111.162.4	240
117.21.246.164	390
118.142.68.222	184
12.130.60.4	454
12.130.60.5	310
121.254.179.199	366
121.9.245.177	324

Nuova ricerca

Salva come ▾ Crea vista tabella Chiudi

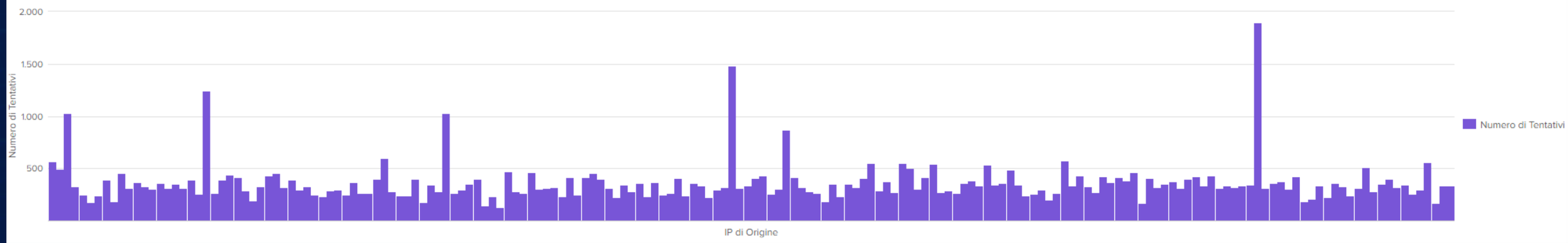
```
source="tutorialdata.zip:*" sourcetype="www1/secure" | rex "Failed password for .* from (?<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"
| stats count as num_attempts by src_ip
| where num_attempts > 5
| table src_ip num_attempts
| rename src_ip as "IP di Origine", num_attempts as "Numero di Tentativi"
```

Sempre ▾

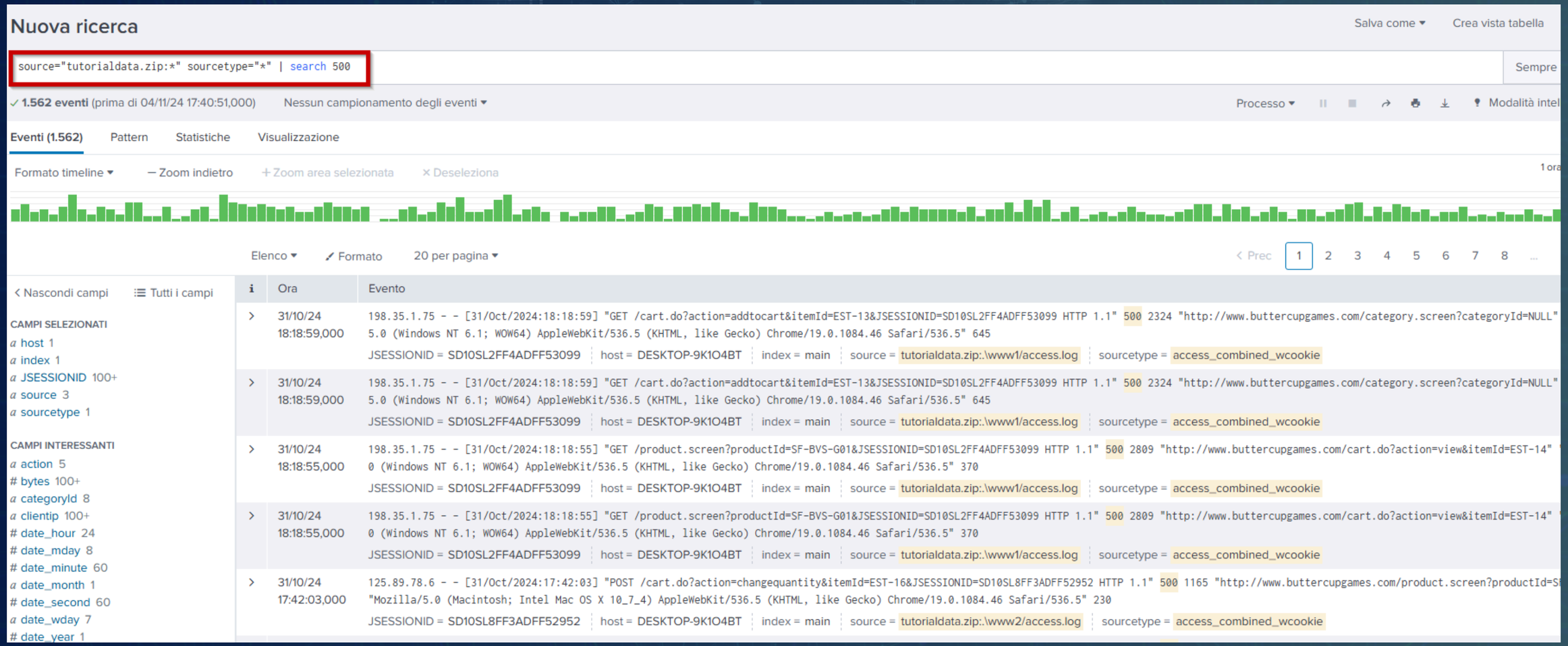
✓ **80.176 eventi** (prima di 04/11/24 17:37:37,000) Nessun campionamento degli eventi ▾ Processo ▾ Modalità intelligente ▾

Eventi Pattern Statistiche (182) Visualizzazione

Grafico a colonne Formato Trellis



Crea una query Splunk per trovare tutti gli Internal Server Error.



Conclusioni sui log analizzati utilizzando AI.

Conclusione Generale:

Le informazioni nei log mostrano un comportamento che potrebbe suggerire tentativi di accesso non autorizzati al sistema. Esistono diversi tentativi di accesso falliti provenienti da vari indirizzi IP e utilizzando nomi di utenti diversi. È inoltre presente almeno un accesso riuscito per un utente specifico. Ecco una panoramica dettagliata.

Prima Immagine (First_Query.png)

1.Tentativi di Accesso Falliti:
- Ci sono numerosi eventi di "Failed password", che indicano tentativi di accesso falliti.
- Ogni tentativo utilizza nomi di utenti diversi come "appserver", "testuser", "mongodb", "desktop", "cyrus".
- L'indirizzo IP di origine di questi tentativi è 194.8.74.23.

2. Possibile Brute-Force:
- L'utilizzo di più nomi utente suggerisce un possibile attacco brute-force o tentativi di accesso non autorizzati. L'attaccante potrebbe star cercando di indovinare una combinazione valida di nome utente e password.

3. Comportamento dell'indirizzo IP 194.8.74.23:
- Questo IP sembra essere persistente nei tentativi di accesso falliti e potrebbe rappresentare un'attività sospetta. Dato il numero di tentativi e la varietà di utenti, è possibile che questo IP sia parte di un attacco.

Seconda Immagine (Second_Query.png)

1. **Accesso Riuscito per djohnson:**
   - In questa query, osserviamo che l'utente djohnson è riuscito ad aprire una sessione sul sistema.
   - L'evento mostra il processo sshd che segnala "session opened for user djohnson", il che implica che l'autenticazione è stata completata con successo.

2. **Accesso Valido vs. Accesso Non Autorizzato:**
   - Questo accesso potrebbe rappresentare un'attività legittima, specialmente perché i log non riportano errori associati. Tuttavia, l’accesso di djohnson potrebbe dover essere verificato per assicurarsi che provenga da una fonte sicura, specialmente in un contesto dove ci sono tentativi di accesso falliti da altri utenti.

3. **Monitoraggio di djohnson:**
   - Dato il contesto di accessi falliti, potrebbe essere utile monitorare ulteriori accessi dell'utente djohnson per assicurarsi che non sia stato compromesso.

Terza Immagine (Tirthd_query.png)

1. Attività Sospetta dall'IP 86.212.199.60:
    - Ci sono diversi tentativi di accesso falliti provenienti dall'IP 86.212.199.60.
    - Questi tentativi coinvolgono vari utenti (es. "agusto", "tomcat", "desktop", "yp") e diverse porte SSH, il che potrebbe indicare che l’attaccante sta testando diverse combinazioni di porta e utente.

2. Possibile Attacco Distribuito su Porte Diverse:
    - L'uso di varie porte SSH per tentativi di accesso potrebbe essere un tentativo di aggirare eventuali sistemi di protezione, come firewall o sistemi di rilevamento di intrusione (IDS).
    - Questo comportamento, unito alla varietà di utenti, rafforza l'ipotesi di un attacco brute-force o di un attacco a dizionario, in cui l'attaccante cerca di accedere con diverse combinazioni di credenziali.

Quarta Query (Tentativi di accesso falliti)

- Sono presenti diversi indirizzi IP con un numero molto elevato di tentativi di accesso falliti, alcuni con centinaia e persino migliaia di tentativi.
- Questo è un possibile indicatore di attacchi brute-force, dove un attaccante cerca di indovinare le credenziali di accesso eseguendo tentativi ripetuti.
- Raccomandazione: Bloccare temporaneamente gli IP con alto numero di tentativi o implementare una soluzione di "rate limiting" che riduca la possibilità di attacchi brute-force. Inoltre, sarebbe opportuno implementare meccanismi di allarme quando un IP supera un certo numero di tentativi falliti.
- IP da monitorare: Alcuni IP, come 109.169.32.135 e 107.3.146.207, hanno un numero particolarmente alto di tentativi (1030 e 564 rispettivamente), richiedendo un monitoraggio specifico.

Quinta Query (Errori di server - Codice HTTP 500)

- Ci sono numerosi errori 500 nei log, suggerendo problemi con il server o con l’applicazione stessa. Gli errori 500 sono generalmente legati a malfunzionamenti interni che impediscono al server di completare una richiesta.
- Alcuni URL specifici, come /cart.do?action=addtocart e /category.screen, sembrano particolarmente colpiti dagli errori. Questo potrebbe indicare problemi con il codice relativo al carrello o alle pagine di categoria del sito.
- Implicazioni per l’esperienza utente: La presenza di numerosi errori 500 può influire negativamente sull’esperienza dell’utente, in quanto questi non riuscirebbero a completare determinate azioni (es. aggiungere articoli al carrello).
- Raccomandazione: Analizzare e correggere il codice delle pagine che mostrano frequentemente errori 500. Potrebbe essere necessario anche un test di carico per assicurarsi che il server possa gestire richieste multiple senza andare in errore.

Conclusioni Generali

1. **Possibile Attacco Brute-Force o Tentativi di Accesso Non Autorizzati:**
   - **Sia l'IP 194.8.74.23 che 86.212.199.60 mostrano segni di tentativi di accesso ripetuti e falliti con diversi nomi utente. Questo pattern è tipico di un attacco brute-force.**

1. **Indirizzi IP da Monitorare:**
   - **Gli IP 194.8.74.23 e 86.212.199.60 sono sospetti e dovrebbero essere monitorati attentamente. Potrebbe essere opportuno bloccarli temporaneamente per prevenire ulteriori tentativi di accesso.**

3. Controllo delle Credenziali di djohnson:

- L'accesso riuscito dell'utente djohnson dovrebbe essere verificato per assicurarsi che sia stato effettuato da una fonte sicura. Considerando che ci sono stati numerosi tentativi falliti di altri utenti, esiste un rischio che account legittimi possano essere stati compromessi.

4. Implementare Sistemi di Difesa:

- Sistemi come blocco temporaneo degli IP dopo un certo numero di tentativi falliti, o implementazione di autenticazione a due fattori, potrebbero aiutare a mitigare questi tentativi di accesso non autorizzato.
- Considerare di limitare l'accesso SSH a indirizzi IP conosciuti e fidati, se applicabile, oppure configurare firewall per filtrare tentativi di accesso non autorizzati su porte non standard.

5. Problemi di sicurezza:

- I tentativi di accesso falliti multipli da parte di certi IP suggeriscono attività sospette, possibilmente attacchi brute-force. È necessario implementare contromisure di sicurezza per limitare tali tentativi.

6. Problemi di affidabilità:

- Gli errori 500 ricorrenti su determinati endpoint suggeriscono instabilità o malfunzionamenti a livello applicativo, che potrebbero richiedere un debugging approfondito e potenziali ottimizzazioni del codice.

Filippo Lucchetti

THANK YOU!