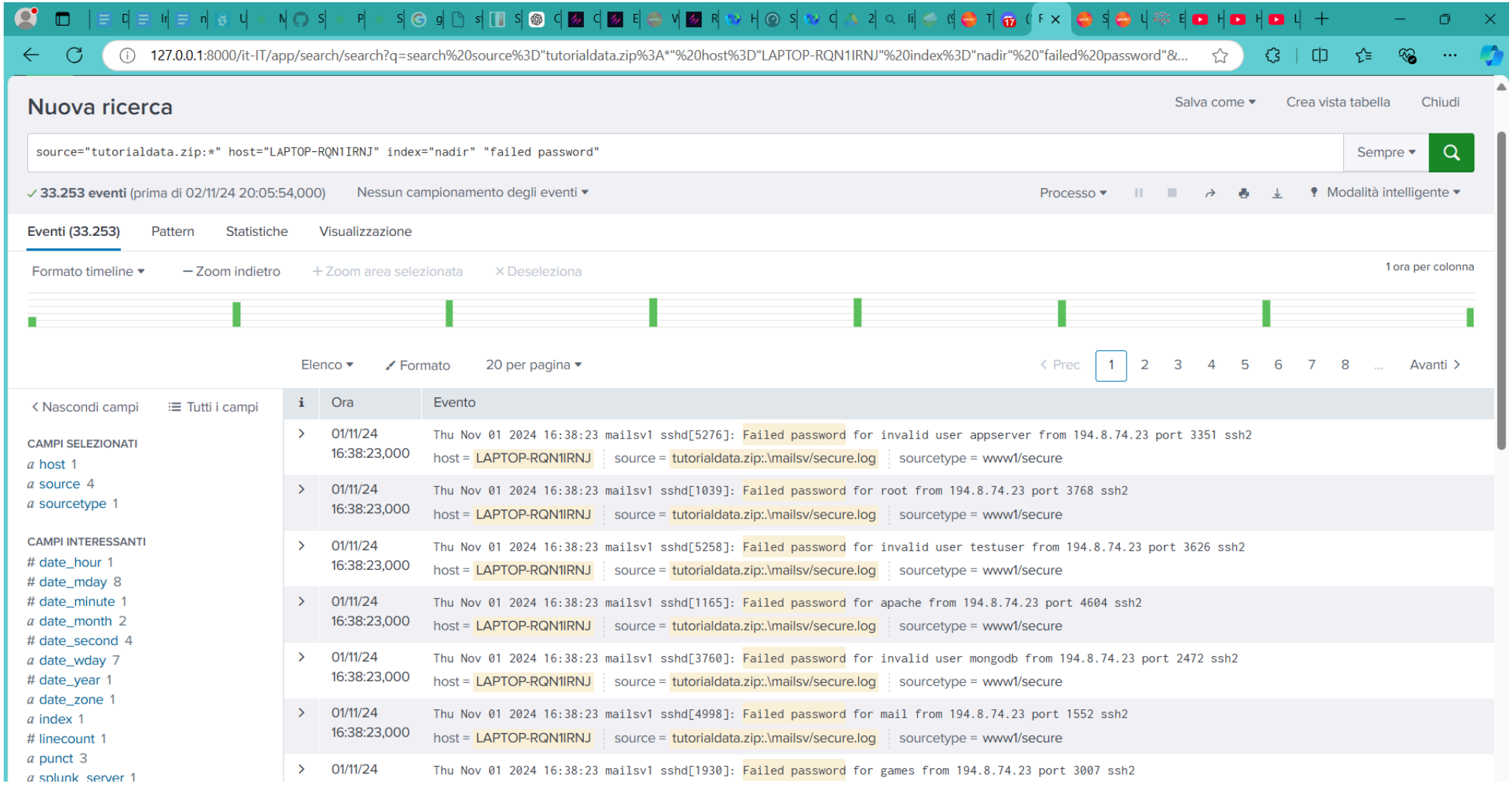
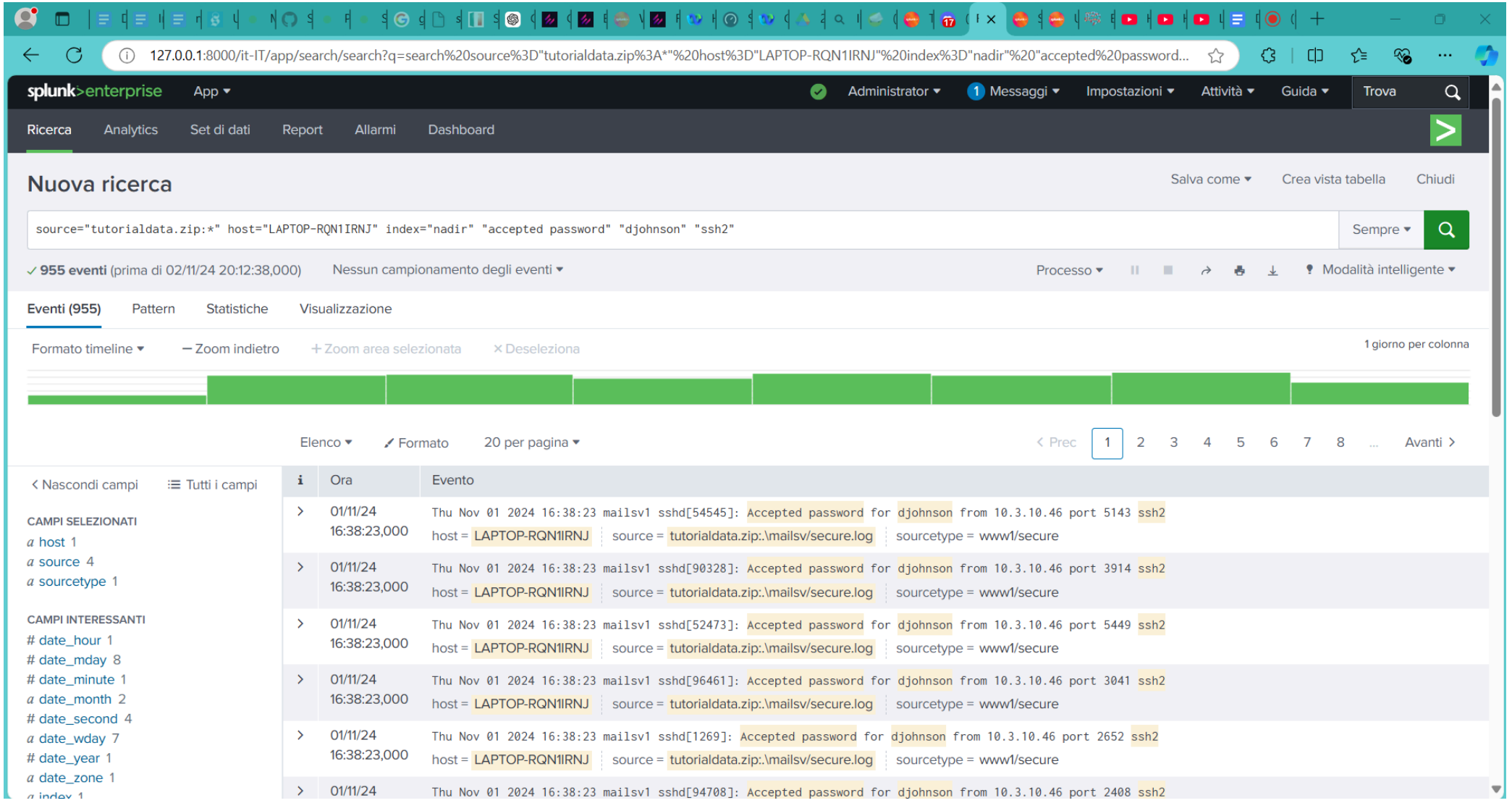
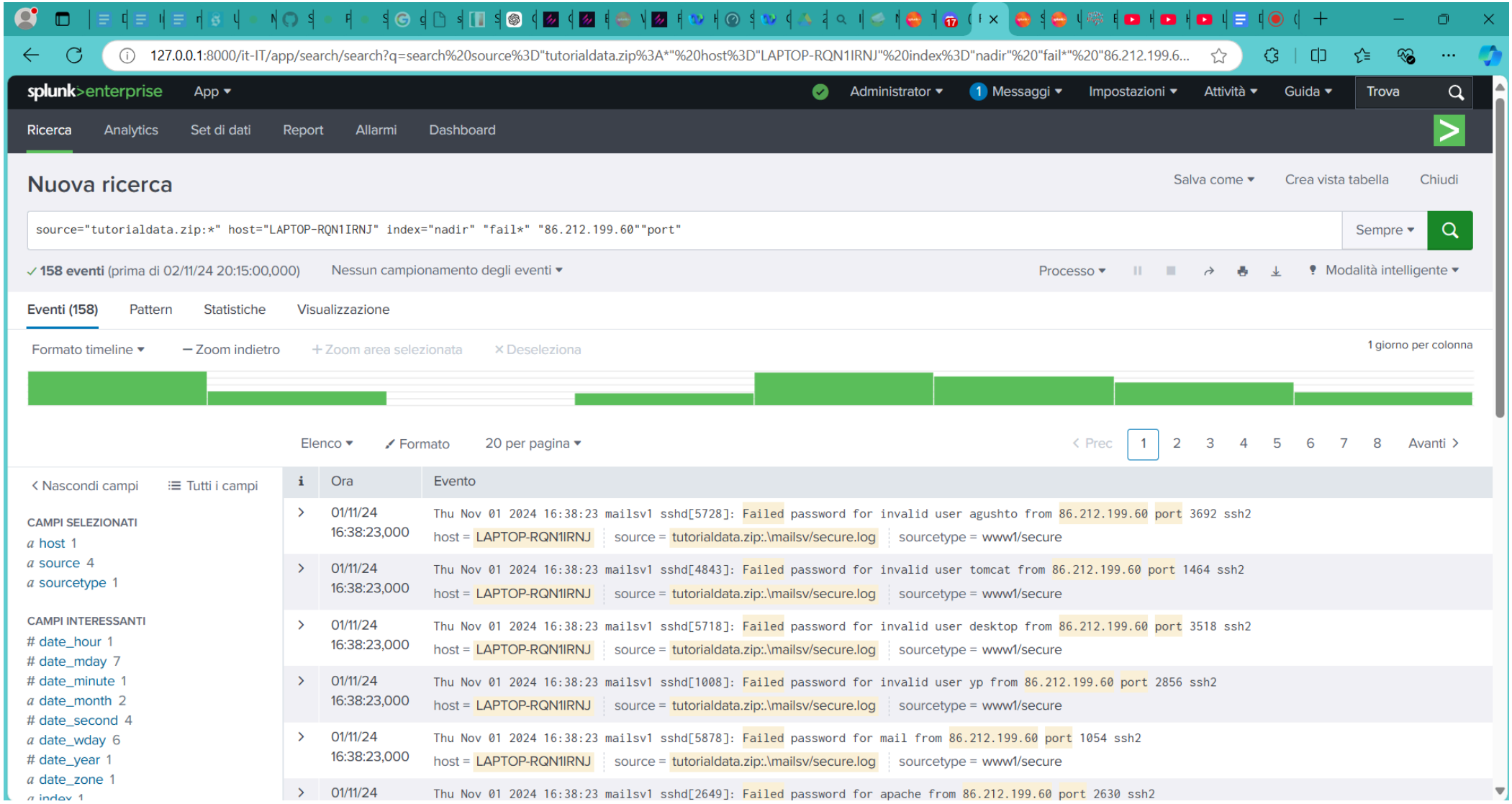
Trovare Failed Password



Trovare richieste accettate con l'utente *djohnson*

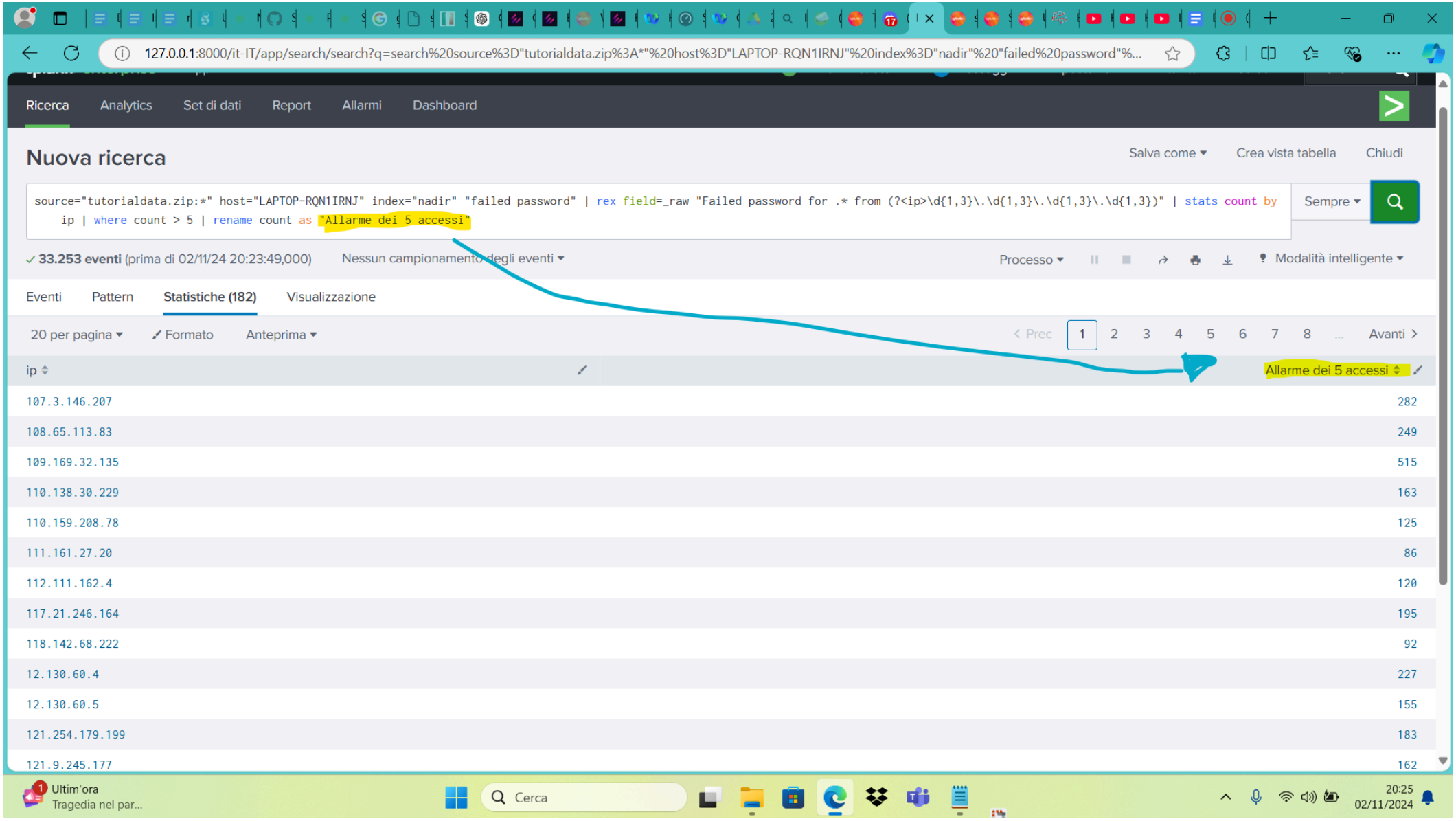


Trovare richieste fallite associate all'indirizzo 86.212.199.60



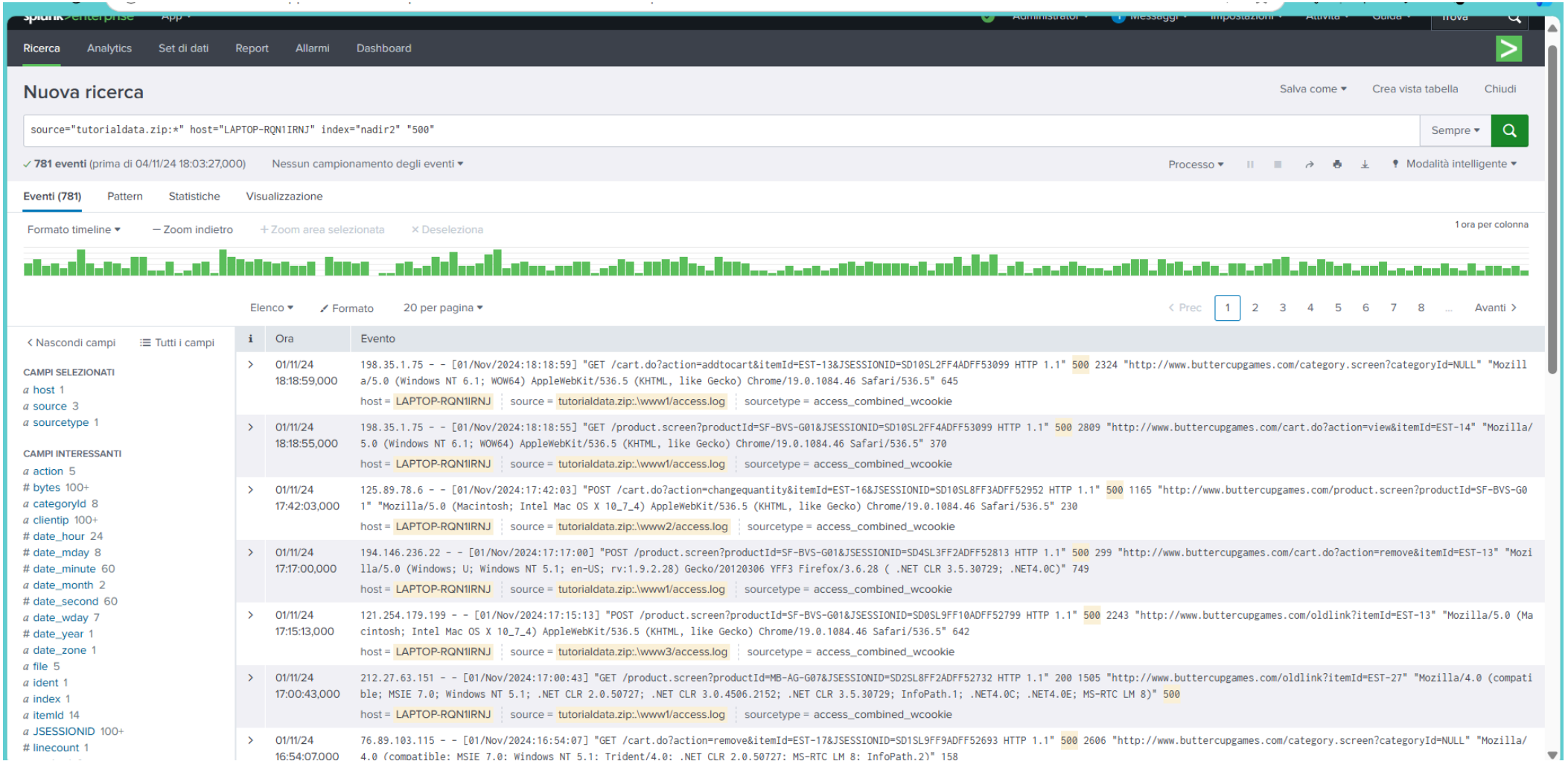
Trovare IP che hanno tentato di accedere più di 5 volte

Ho elaborato una *query* che indicasse a Splunk di individuare tutte quelle stringhe che, per numero e ordine di caratteri, hanno la struttura di un indirizzo IP, dando ad esse il nome “ip”. Solo allora ho potuto chiedere a Splunk di contare gli accessi da parte di quegli IP e mostrarmi quelli maggiori di 5 nel tag “Allarme dei 5 accessi”..



Internal Server Error

Gli internal server error, sono identificati dal codice di stato HTTP 500, quindi mi basta specificarlo nella query



Trarre conclusioni utilizzando AI.

CON L'AIUTO DI CHAT-GPT HO PROVATO A FORMULARE DELLE IPOTESI SUI DATI RACCOLTI E FILTRATI

1. **Tentativi di accesso falliti**:
    - Diversi log mostrano ripetuti tentativi di accesso falliti tramite SSH (come evidenziato dai messaggi "Failed password"). Questi potrebbero indicare tentativi di brute-force o attacchi di credential stuffing. L'elevato numero di tentativi di accesso falliti provenienti da diversi indirizzi IP potrebbe indicare un attacco distribuito, in cui più attori o botnet tentano simultaneamente di accedere al sistema per bypassare le misure di protezione basate sul rilevamento da singolo IP
    - La presenza di indirizzi IP specifici che effettuano molti tentativi suggerisce attività sospette provenienti da possibili attori malevoli che tentano di accedere senza autorizzazione.
2. **Tentativi di accesso riusciti**:
    - Alcuni log riportano accessi accettati (come evidenziato da "Accepted password"), indicando che ci sono connessioni SSH andate a buon fine, potenzialmente legittime, ma che devono essere analizzate per confermare l'autenticità degli utenti.
3. **Indirizzi IP sospetti**:
    - Sono stati identificati indirizzi IP che hanno eseguito molti tentativi di accesso falliti. In uno screenshot specifico, si osserva che ci sono IP con un numero considerevole di tentativi non riusciti (es. 282, 249, 515 eventi). Questi IP potrebbero essere inclusi in una lista di blocco temporanea o permanente per proteggere il sistema.
4. **Accessi ripetuti e frequenti**:
    - La visualizzazione dei log mostra una frequenza elevata di tentativi di connessione da parte di indirizzi IP specifici. La quantità di tentativi superiori a una soglia (come il filtro che identifica gli "allarmi dei 5 accessi") evidenzia un'attività anomala che dovrebbe essere monitorata attentamente.
5. **Log di errore HTTP 500**:
    - Alcuni log indicano errori HTTP 500, che possono rappresentare malfunzionamenti nei servizi web o potenziali tentativi di attacco, come vulnerabilità di tipo DoS (Denial of Service) o attacchi mirati che provocano errori server-side.

Ipotesi di rischio per la sicurezza:

- **Attacchi Brute-force**: L'elevato numero di tentativi di accesso falliti da vari IP suggerisce un attacco brute-force in corso, volto a ottenere l'accesso non autorizzato ai sistemi.
- **Compromissione di Credenziali**: Se gli accessi accettati provengono da IP non riconosciuti o insoliti, potrebbe indicare che alcune credenziali sono state compromesse.
- **Test di Vulnerabilità**: Gli errori HTTP 500 potrebbero essere il risultato di attacchi per individuare vulnerabilità o tentativi di sfruttamento di difetti nel software del server.
- **Potenziale Escalation**: Se un attaccante è riuscito a ottenere l'accesso con credenziali valide (come indicato dai tentativi di accesso riusciti), potrebbe tentare di eseguire un'escalation dei privilegi per aumentare il controllo sul sistema.

Raccomandazioni:

- **Blocco IP**: Implementare un blocco IP temporaneo per gli indirizzi con attività sospette.
- **Monitoraggio attivo**: Incrementare il livello di monitoraggio e correlare questi eventi con altri dati di log per rilevare schemi di comportamento dannoso.
- **Analisi delle credenziali**: Verificare se gli accessi accettati sono stati eseguiti da utenti noti o se sono il risultato di credenziali compromesse.
- **Patch e aggiornamenti**: Assicurarsi che il sistema sia aggiornato per mitigare potenziali vulnerabilità sfruttabili.