REPORT ESERCIZIO W24D4

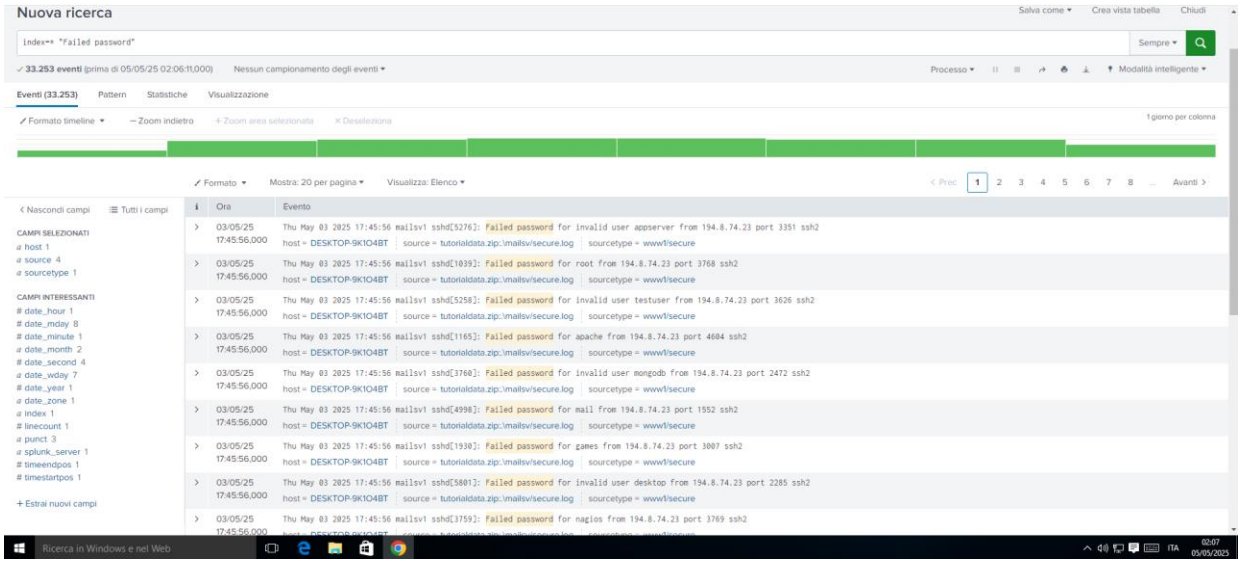
Report Analisi Log Splunk
In questo report vengono presentate le analisi di sicurezza eseguite tramite **Splunk** su un dataset di log estratti dal file **tutorialdata.zip.** Sono state realizzate **5 query** mirate per identificare comportamenti sospetti, tentativi di accesso falliti, sessioni SSH, errori HTTP e attività anomale da parte di IP specifici.

Conclusioni AI-based

Dall'analisi dei Log sono emerse diverse evidenze significative:

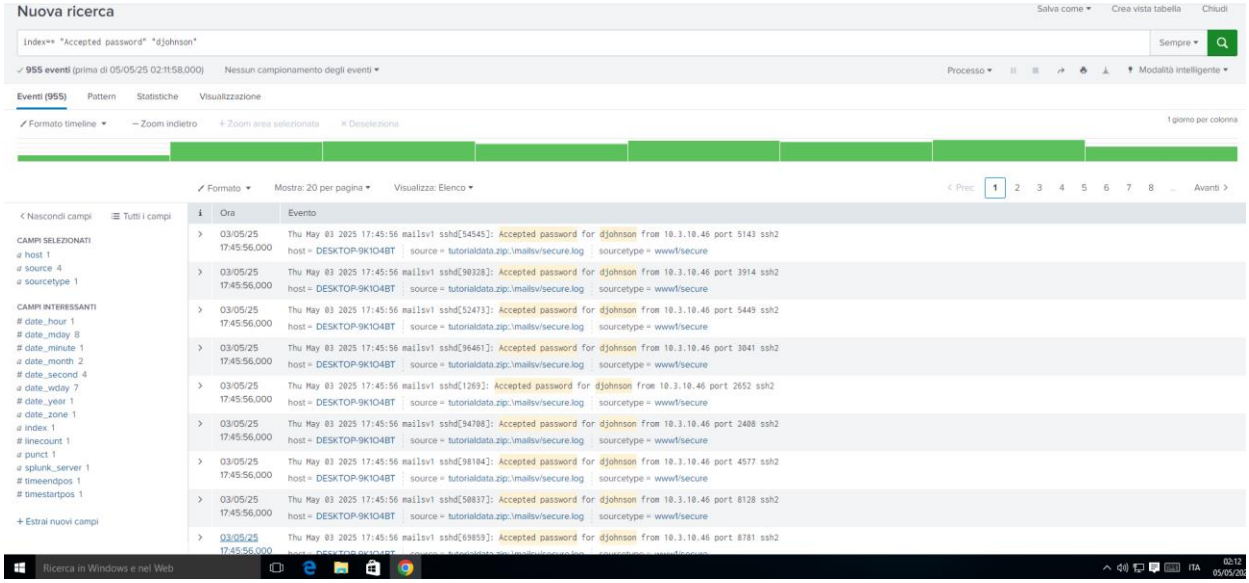
1. Tentativi di accesso falliti:

Numerosi eventi contengono messaggi di **'Failed password'**, soprattutto da utenti non validi. Questo suggerisce attività di brute-force o attacchi automatizzati su SSH.



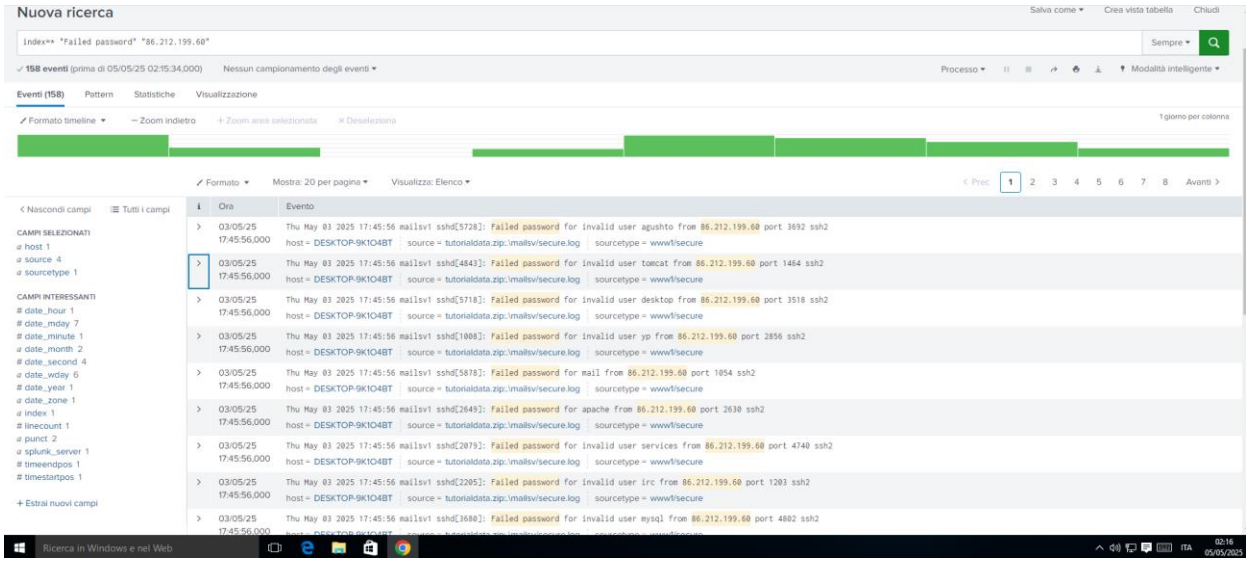
2. Accessi SSH riusciti dell'utente djohnson:

Sono stati registrati molti login riusciti da parte di questo utente, tutti da un singolo IP, il che può indicare attività legittima o un account compromesso sfruttato da un solo host.



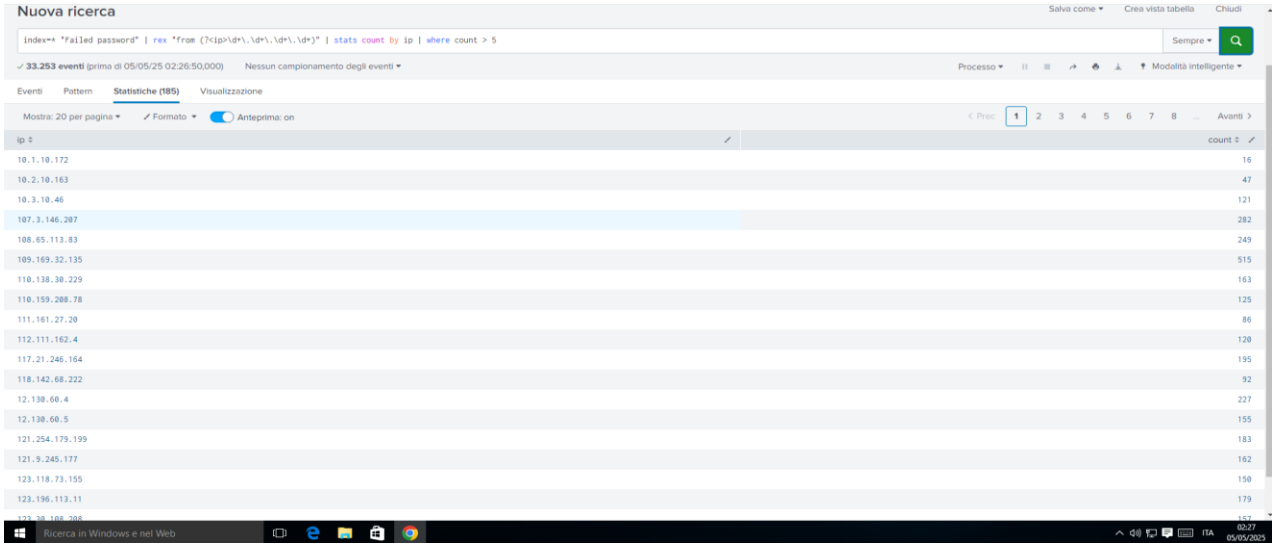
3. Attacchi mirati da un IP specifico:

L'indirizzo **IP 86.212.199.60** ha generato numerosi tentativi falliti, usando diversi username e porte. Questo comportamento è tipico di uno scanner automatico.



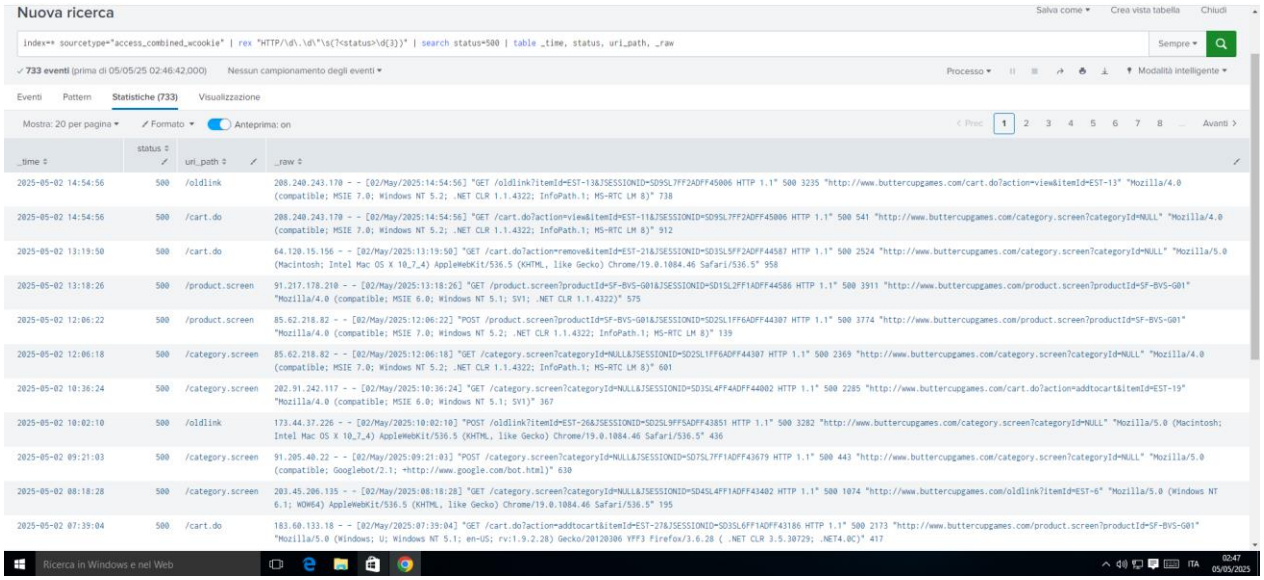
4. Elenco di IP ostili:

Sono stati identificati più di 100 indirizzi IP che hanno tentato l’accesso fallendo oltre 5 volte. Questi IP potrebbero essere inseriti in una blacklist o sottoposti a sistemi di throttling.



5. Errori 500 - Internal Server Error:

Diversi endpoint dell’applicazione web (come /cart.do e /product.screen) generano errori 500, il che potrebbe indicare problemi lato server, vulnerabilità o carichi anomali da automatismi.



Conclusione finale:

I Log analizzati evidenziano pattern coerenti con un contesto di rete esposta, probabilmente soggetta a tentativi di scansione, brute-force e potenziali vulnerabilità web.

Si raccomanda di applicare controlli su IP sospetti, implementare sistemi IDS/IPS e monitorare costantemente endpoint critici con alert automatici.