ANALISI LOG

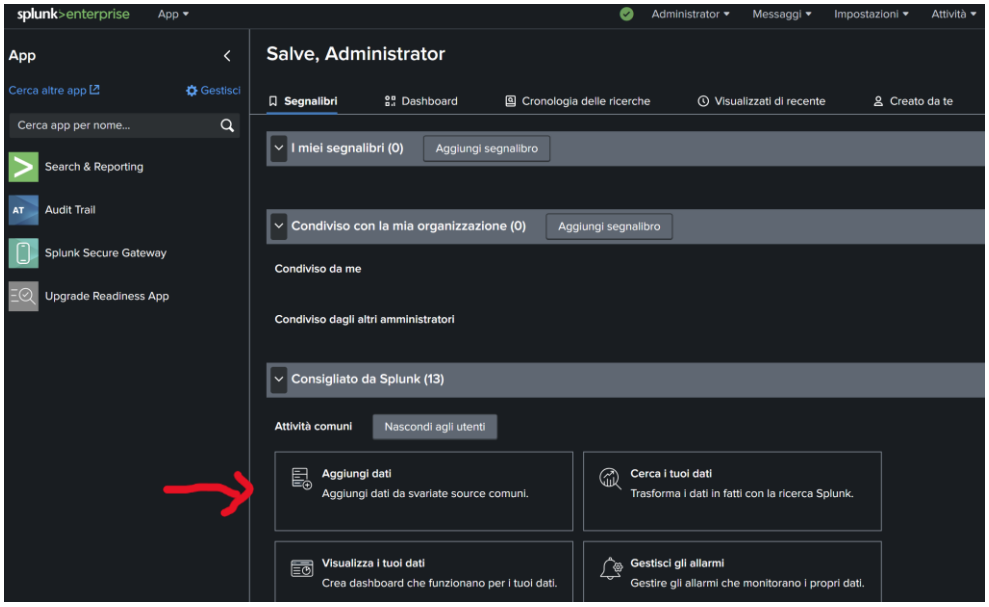
10/02/2025

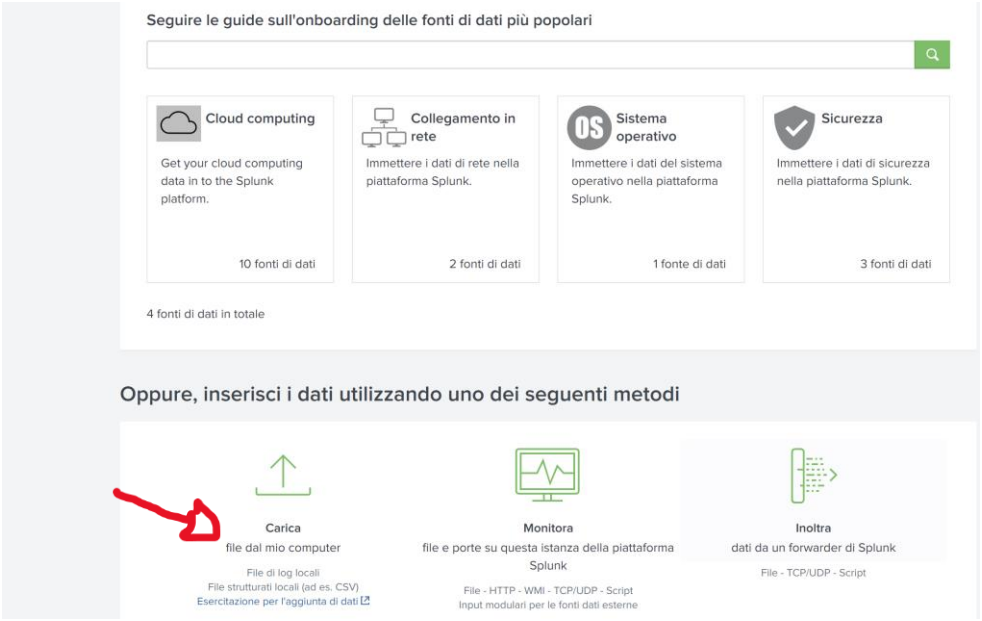
TRACCIA

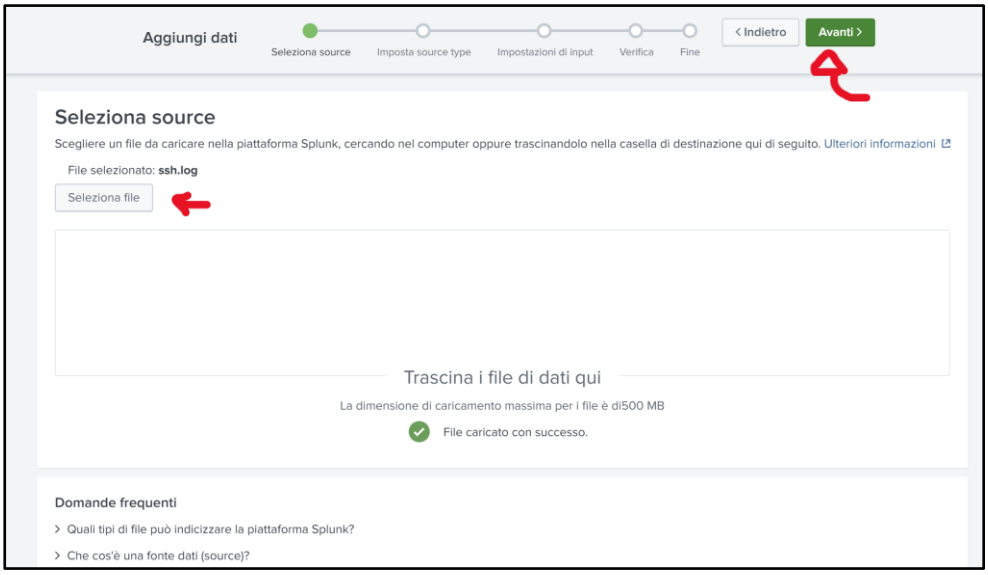
Analizzare il log ssh.log fornito e indicare elementi rilevanti, ovvero login falliti, tentativi di attacco ecc.

SVOLGIMENTO

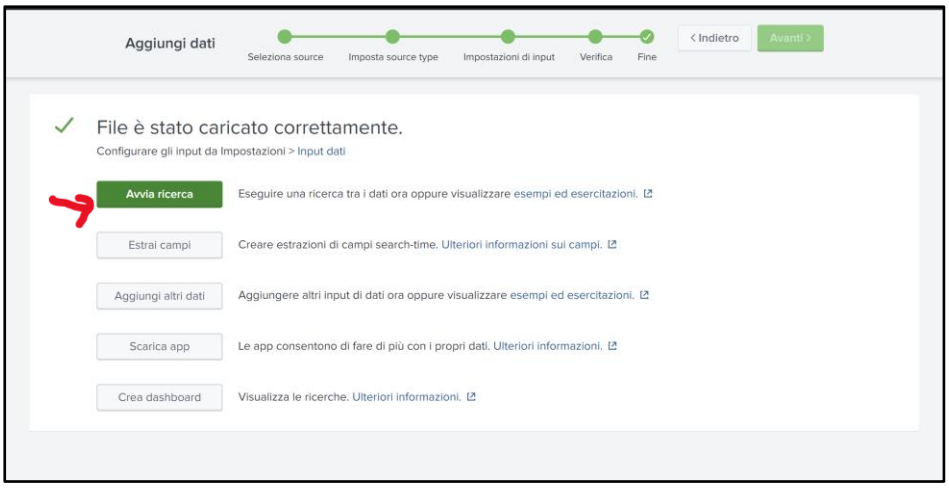
Apriamo splunk e carichiamo il nostro file:



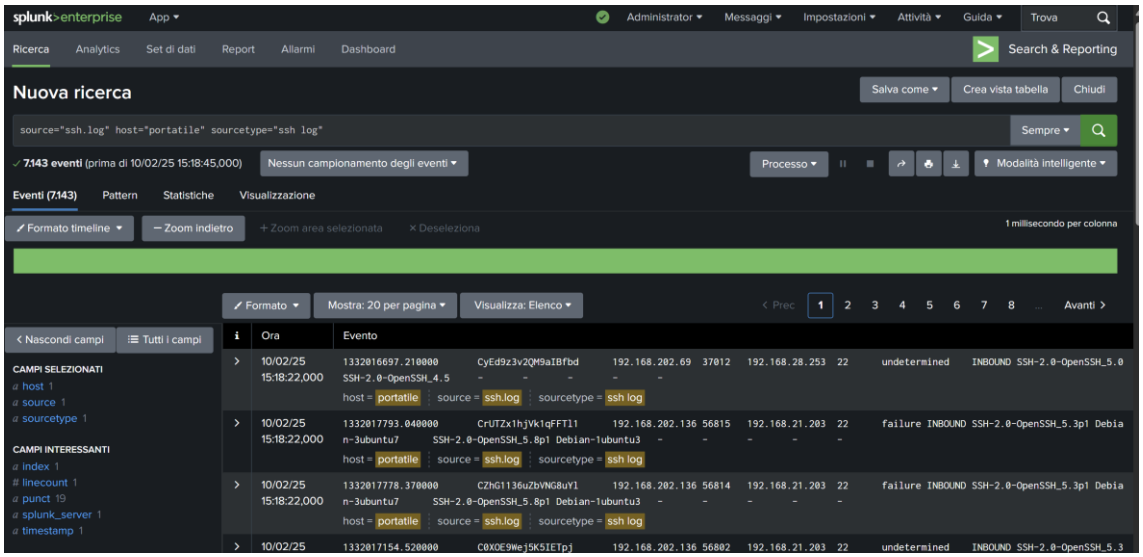




Andiamo avanti fino alla fine del caricamento

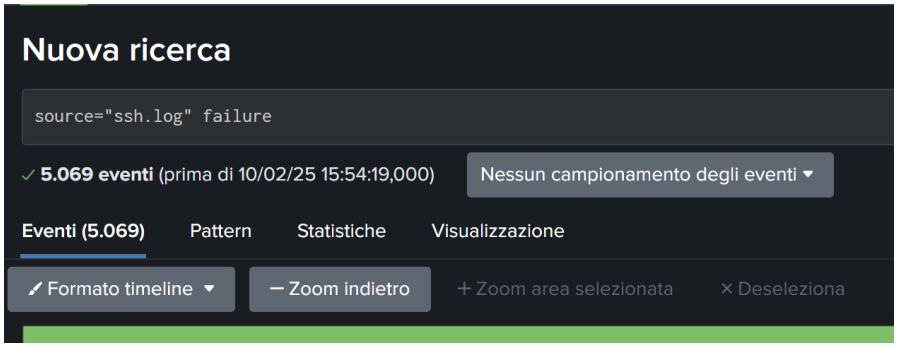


Una volta caricato il file, avremo una schermata del genere



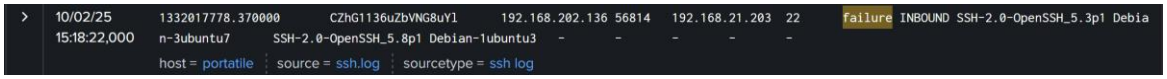
Possiamo vedere tutti gli eventi; a sinistra c’è il numero totale (7143).

Filtriamo gli eventi con <failure> poichè non ci interessano quelli con successo.



Gli eventi sono 5069, quindi abbiamo 5069 tentativi di accesso falliti.

Analizziamo un log:



10/02/25 15:18:22,000

Tentativo di connessione avvenuto il **10 Febbraio 2025 alle 15:18:22**

1332017778.370000

Timestamp della connessione, standardizzato in secondi

CZhG1136uZbVNG8uYl

Identificativo univoco della sessione SSH

192.168.202.136

L'indirizzo IP che ha tentato di connettersi

56814

Porta utilizzata dall'host di origine per connettersi

192.168.21.203

L'indirizzo IP del server di destinazione

22

La connessione è stata diretta alla **porta 22**, usata dal servizio SSH

Failure

l tentativo di connessione **è fallito**, indicando possibili attacchi brute-force o credenziali errate

INBOUND

Si tratta di un tentativo di connessione in entrata

SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7

La versione SSH usata dal client (attaccante)

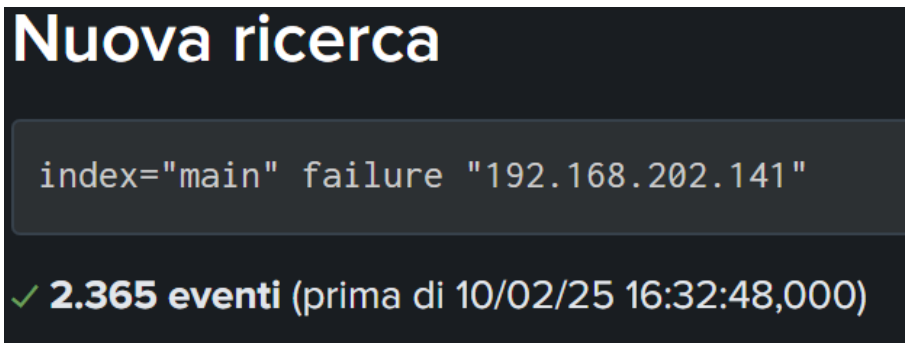
SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3

La versione SSH del server di destinazione

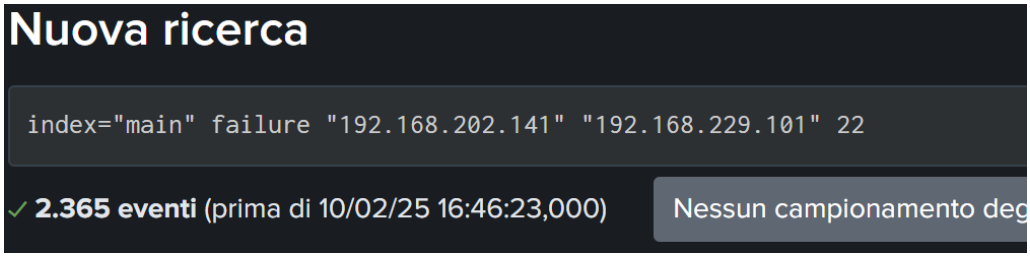
Portatile

Nome del dispositivo che ha generato il log

Ci sono diversi indirizzi IP che hanno tentato di connettersi, quello con più tentativi falliti è il 192.168.202.141



Possiamo notare che la maggior parte dei tentativi, se non tutti sono diretti verso **192.168.229.101** sulla porta **22.**



Questo comportamento può signifcare 2 cose:

1. Attacco di Brute Force SSH

2. Scansione di Rete

Il grande numero di tentativi falliti in un breve periodo suggerisce che qualcuno (o un bot) stia cercando di forzare l'accesso a **192.168.229.101** con credenziali casuali. Questo è spesso il primo passo di un attacco, per poi decidere se eseguire brute force o sfruttare una vulnerabilità.

Se non ci sono tentativi di autenticazione ma solo connessioni rifiutate, potrebbe trattarsi di **ricognizione** tramite un tool come **Nmap**, cercando di identificare la versione del server SSH e le sue configurazioni. Questo è spesso il **primo passo di un attacco**, per poi decidere se eseguire brute force o sfruttare una vulnerabilità.