

ANALISI LOG

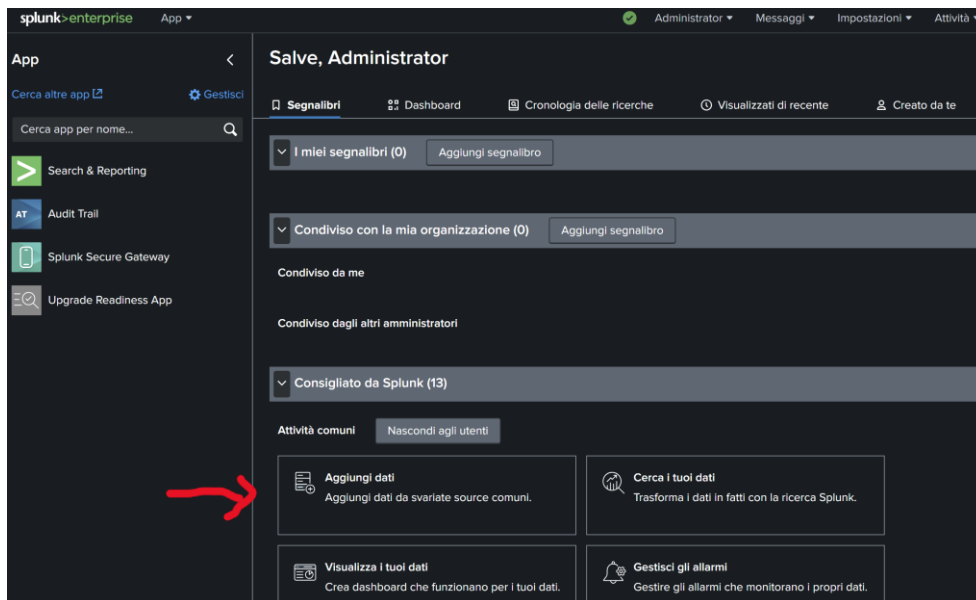
10/02/2025

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:



Seguire le guide sull'onboarding delle fonti di dati più popolari

Cloud computing
Get your cloud computing data in to the Splunk platform.
10 fonti di dati

Collegamento in rete
Immettere i dati di rete nella piattaforma Splunk.
2 fonti di dati

Sistema operativo
Immettere i dati del sistema operativo nella piattaforma Splunk.
1 fonte di dati

Sicurezza
Immettere i dati di sicurezza nella piattaforma Splunk.
3 fonti di dati

4 fonti di dati in totale

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

Aggiungi dati

Selezione source Imposta source type Impostazioni di input Verifica Fine

< Indietro **Avanti >**

Selezione source

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

File selezionato: **ssh.log**

Seleziona file

Trascina i file di dati qui

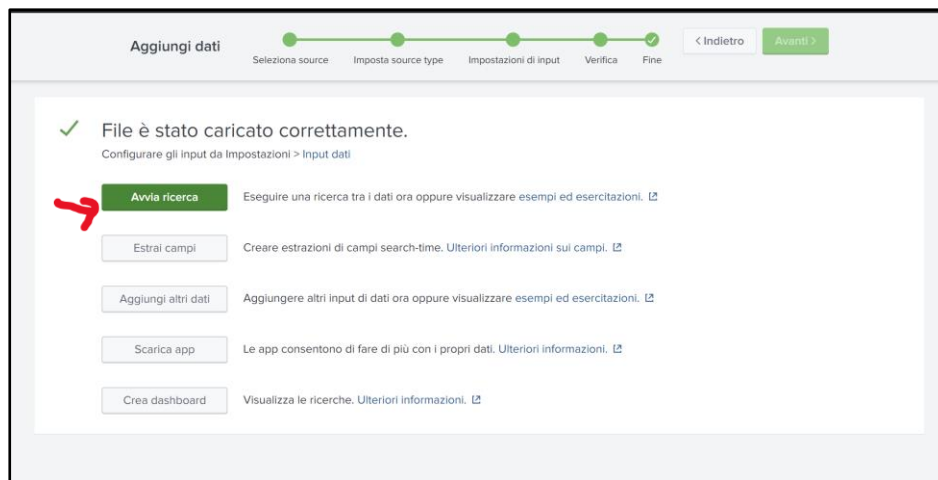
La dimensione di caricamento massima per i file è di 500 MB

File caricato con successo.

Domande frequenti

- > Quali tipi di file può indicizzare la piattaforma Splunk?
- > Che cos'è una fonte dati (source)?

Andiamo avanti fino alla fine del caricamento



Una volta caricato il file, avremo una schermata del genere

Nuova ricerca

source="ssh.log" host="portatile" sourcetype="ssh log"

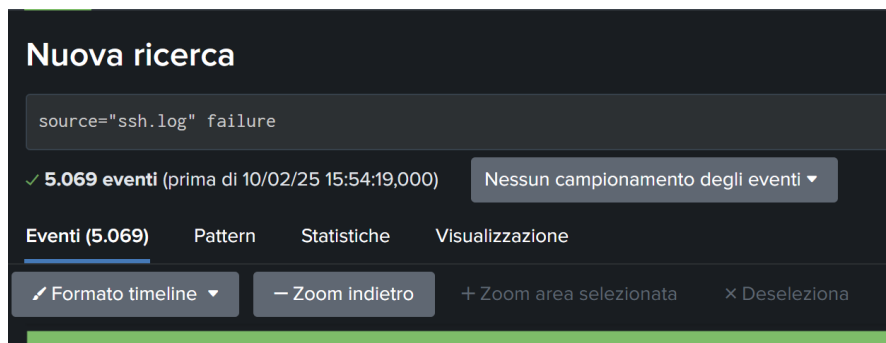
7143 eventi (prima di 10/02/25 15:18:45,000) Nessun campionamento degli eventi

Formato timeline Zoom indietro Zoom area selezionata Deselezione 1 millisecondo per colonna

i	Ora	Evento
>	10/02/25 15:18:22,000	1332016697.210000 CyEd9z3v2QH9aIBfbd 192.168.202.69 37012 192.168.28.253 22 undetermined INBOUND SSH-2.0-OpenSSH_5.0
>	10/02/25 15:18:22,000	1332017793.040000 CrUTz1h3VklqFT11 192.168.202.136 56815 192.168.21.203 22 failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debia
>	10/02/25 15:18:22,000	1332017778.370000 CZHG1136uZbVNG8uY1 192.168.202.136 56814 192.168.21.203 22 failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debia
>	10/02/25 15:18:22,000	1332017154.520000 C0X0E9We15K51ETpj 192.168.202.136 56802 192.168.21.203 22 undetermined INBOUND SSH-2.0-OpenSSH_5.3

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	1332017778.370000 n-3ubuntu7	CZhG1136uZbVNG8uYl SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	192.168.202.136 56814	192.168.21.203 22	Failure	INBOUND SSH-2.0-OpenSSH_5.3p1 Debia
		host = portatile	source = ssh.log	sourcetype = ssh 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

Il 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

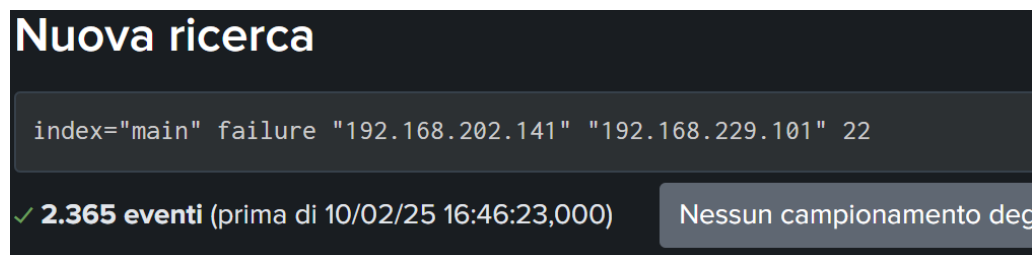
Ci sono diversi indirizzi IP che hanno tentato di connettersi, quello con più tentativi falliti è il **192.168.202.141**

Nuova ricerca

```
index="main" failure "192.168.202.141"
```

✓ **2.365 eventi** (prima di 10/02/25 16:32:48,000)

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



Questo comportamento può significare 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.