

# S10/L1

L'esercizio di oggi consiste nell'analizzare tramite Splunk un log fornitoci dal professore.

Andiamo ad inserire il file all'interno di Splunk lasciando tutte le impostazioni default e ci ritroveremo in questa schermata:

The screenshot shows the Splunk Cloud interface with a search for 'ssh.log' events. The search bar contains the query: `source=\"ssh.log\" host=si-i-02953a1996ad828b2-prd-p-2rhut.splunkcloud.com`. The results show 7143 events. The table displays columns for time, event ID, host, source, sourcetype, and event details. The 'failure' events are highlighted in yellow.

Come vediamo abbiamo più di 7000 eventi essendo che a noi servono elementi irrilevanti come log falliti o tentativi di attacco dobbiamo andare ad utilizzare delle Query precise.

Iniziamo utilizzando questa Query.

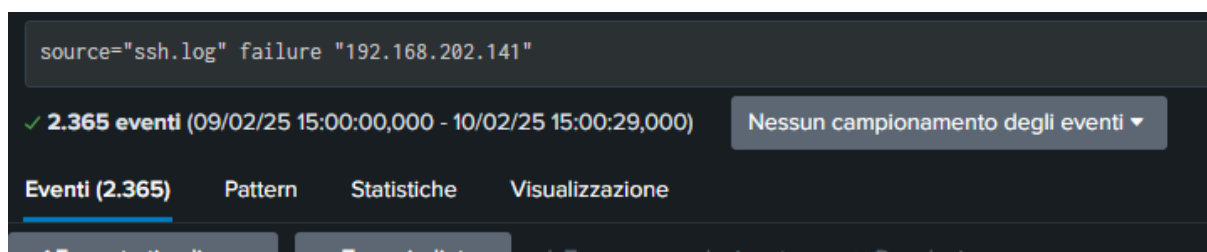
The screenshot shows the Splunk Cloud interface with a search for 'failure' events. The search bar contains the query: `source=\"ssh.log\" failure`. The results show 5,069 events. The table displays columns for time, event ID, host, source, sourcetype, and event details. The 'failure' events are highlighted in yellow.

Come notiamo ora vediamo solo tutte le richieste di login fallite.



192.168.202.141	8000	192.168.229.101	22	failure	INBOUND	-
cloud.com	source = ssh.log	sourcetype = ssh log				
192.168.202.141	7999	192.168.229.101	22	failure	INBOUND	-
cloud.com	source = ssh.log	sourcetype = ssh log				
192.168.202.141	7998	192.168.229.101	22	failure	INBOUND	-
cloud.com	source = ssh.log	sourcetype = ssh log				
192.168.202.141	7997	192.168.229.101	22	failure	INBOUND	-
cloud.com	source = ssh.log	sourcetype = ssh log				
192.168.202.141	7996	192.168.229.101	22	failure	INBOUND	-
cloud.com	source = ssh.log	sourcetype = ssh log				
192.168.202.141	7995	192.168.229.101	22	failure	INBOUND	-
cloud.com	source = ssh.log	sourcetype = ssh log				
192.168.202.141	7994	192.168.229.101	22	failure	INBOUND	-
cloud.com	source = ssh.log	sourcetype = ssh log				
192.168.202.141	7993	192.168.229.101	22	failure	INBOUND	-
cloud.com	source = ssh.log	sourcetype = ssh log				
192.168.202.141	7992	192.168.229.101	22	failure	INBOUND	-
cloud.com	source = ssh.log	sourcetype = ssh log				
192.168.202.141	7991	192.168.229.101	22	failure	INBOUND	-
cloud.com	source = ssh.log	sourcetype = ssh log				
192.168.202.141	7990	192.168.229.101	22	failure	INBOUND	-
cloud.com	source = ssh.log	sourcetype = ssh log				
192.168.202.141	7989	192.168.229.101	22	failure	INBOUND	-
cloud.com	source = ssh.log	sourcetype = ssh log				
192.168.202.141	7988	192.168.229.101	22	failure	INBOUND	-

Analizzando con questa query notiamo come l'indirizzo IP 192.168.202.141 (attaccante) effettua tantissime prove di login verso l'indirizzo IP 192.168.229.101.



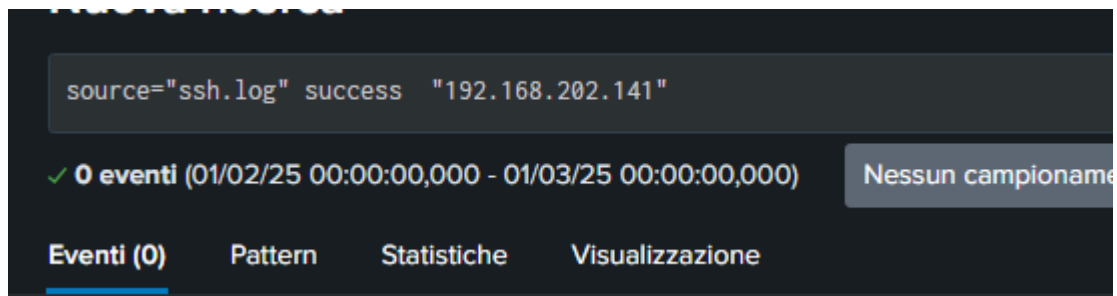
source="ssh.log" failure "192.168.202.141"

✓ 2.365 eventi (09/02/25 15:00:00,000 - 10/02/25 15:00:29,000) Nessun campionamento degli eventi ▼

Eventi (2.365) Pattern Statistiche Visualizzazione

Formato timeline Zoom indietro Zoom avanti Selezione x Deselezione

Come notiamo se inseriamo l'IP dell'attaccante insieme alla scritta failure vediamo che ci sono ben 2365 eventi questo mi fa pensare che questo possa essere stato un attacco brute force a dizionario.



Attacco però che non sembra essere andato a buon fine dato che non troviamo eventi con lo stesso IP dell'attaccante con all'interno la parola success.