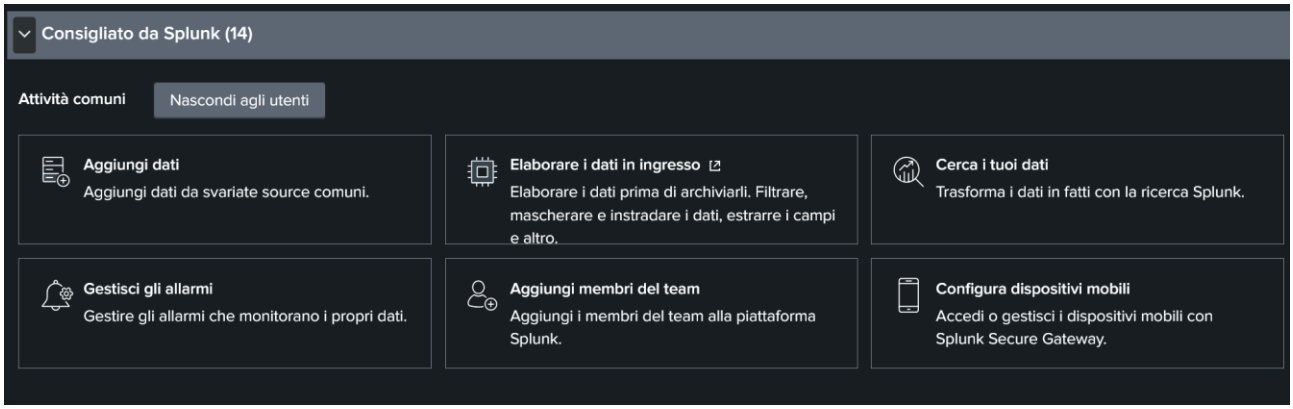
REPORT S10/L1

Analizzare il log ssh.log fornito e indicare elementi rilevanti, ovvero login falliti, tentativi di attacco e trovare tutto ciò che è anomalo.

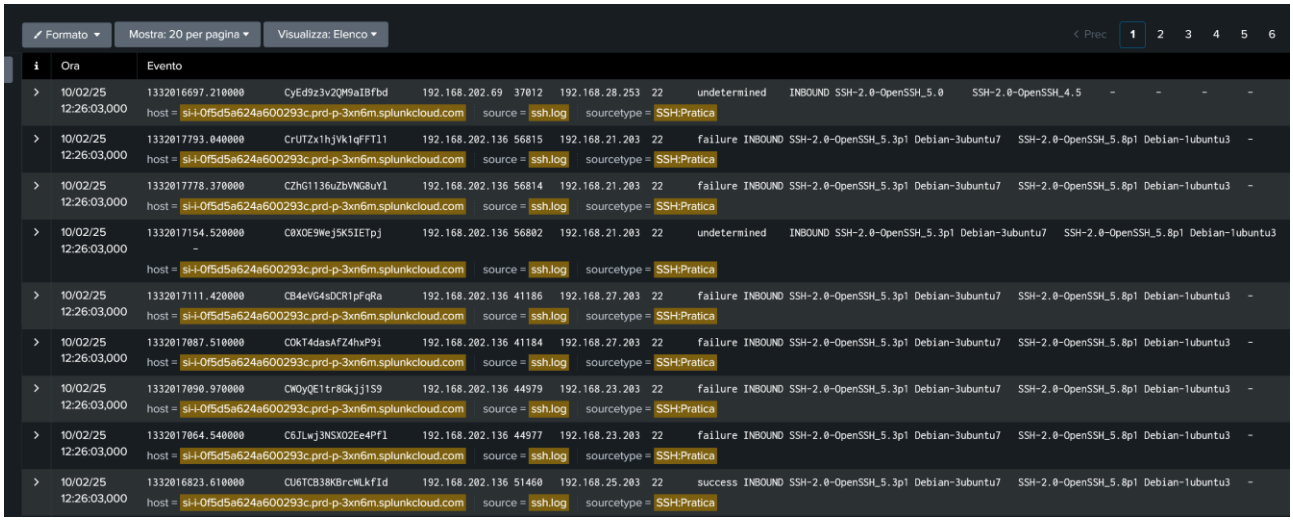
SOLUZIONE

Per prima cosa effettuo l' acceso a Splunk Cloud e procedo selezionando la voce “Aggiungi dati”.



Vado poi nella sezione “Carica” per uploadare il file “ssh.log” trascinandolo nell' apposita sezione.

Dovrei infine avere una schermata come questa.



Posso quindi procedere con l' analisi, vado a filtrare la mia ricerca per i tantativi di login falliti, uso la seguente query:

source="ssh.log" host="si-i-0f5d5a624a600293c.prd-p-3xn6m.splunkcloud.com" sourcetype="SSH:Pratica" "192.168.21.203" failure

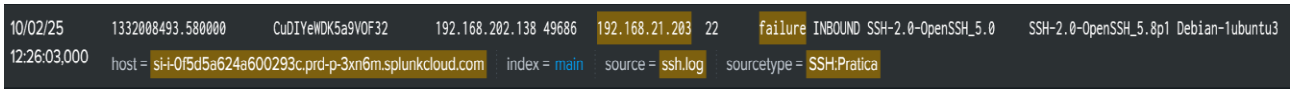
Aggiungo "failure" al termine della stessa in maniera tale da filtrare solo i risultati che evidenziano un tentativo di login fallito. Quello che si nota è quindi un tentantivo di ripetuti tentativi di accesso sul servizio SSH.

Provo ad esaminare una riga per comprenderne meglio il significato.

Quello che emerge in questo caso è quanto segue:

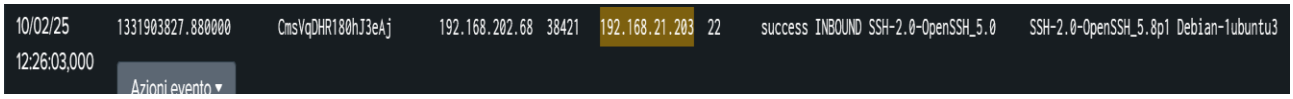
- ***Timestamp*** iniziale che mi indica quando è avvenuto il tentativo di login.
- ***ID Sessione***, identifica la sessione aperta.
- ***IP sorgente*** e porta da cui viene aperta la connesisone.
- ***IP Destinatario*** e porta con la quale si tenta di stabilire la connessione.
- ***Failure***, indica il tentativo di connessione fallita.
- ***INBOUND***, indica il tentantivo di connessione in ingresso.
- ***Nmap-ssh2***, indica che il client ha tentato la connessione mediante nmap.
- ***SSH2.0 openSSH_5.8p1***, è la versione sel servizio ssh sul server destinatario.

Vado ora a vedere le differenze rispetto al caso seguente.



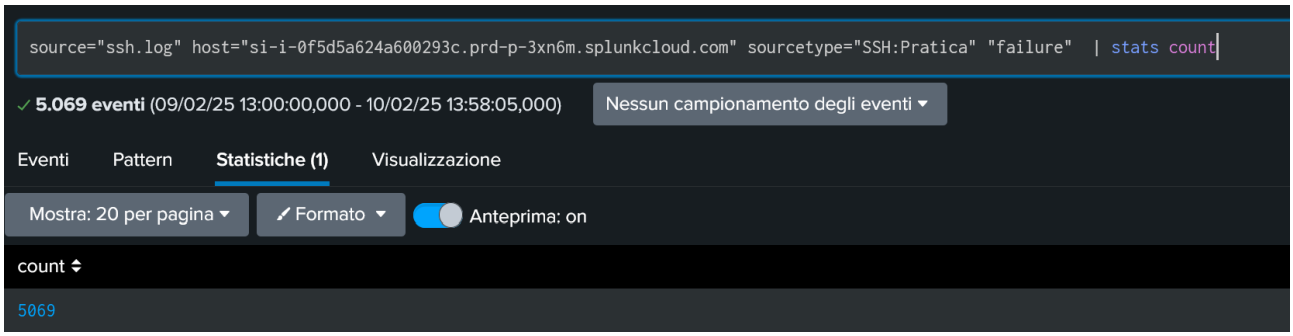
- ***SSH-2.0-OpenSSH_5.0***, versione del servizio SSH che il client sta usando per connettersi.
- ***SSH-2.0:OpenSSH_5.8p1***, versione del servizio SSH verso il quale si tenta la connessione.

Si nota che l' indirizzo ***IP*** dell' attaccante è sempre lo stesso di prima, ***192.168.202.138***, quello che cambia invece è il modo attraverso il quale si tenta la connessione verso il server bersaglio. Nel primo caso infatti questa avveniva mediante una ***Nmap***, quindi mediante un ***tool***, nel secondo caso invece questa avviene attraverso la macchina stessa, è probabile quindi che si sia in presenza di un reale che avviene dopo una scansione.



In questo caso invece si nota come l' esito del tantativo di login si traduca in "***SUCCESS***" a confermare il fatto che l' attaccante sia riuscito ad accedere, è molto probabile quindi che essendo che questo è preceduto da molti tentativi falliti si tratti di un attacco "***brute force***" riuscito. Una cosa che posso fare è a contare le volte che l' IP dell' attaccante ha effettuato dei tentativi di accesso ***SSH*** al server, con la ***query*** che segue:

source="ssh.log" host="si-i-0f5d5a624a600293c.prd-p-3xn6m.splunkcloud.com" sourcetype="SSH:Pratica" "failure" | stats count



Ottengo come risultato che sono stati effettuati 5069 tentativi di accesso falliti dall' attaccante.