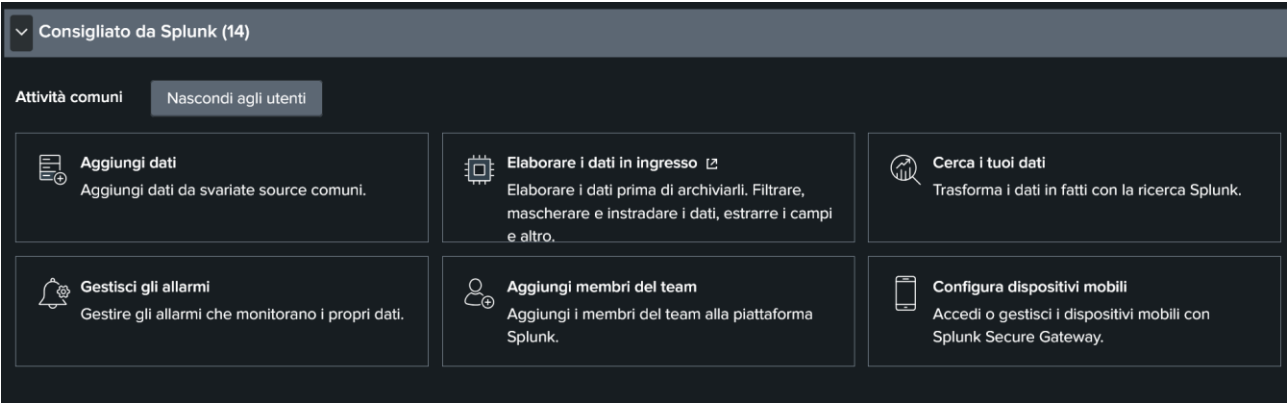


REPORT S10/L1

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'accesso 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.

Formato Mostra: 20 per pagina Visualizza: Elenco											
Prec 1 2 3 4 5 6											
i	Ora	Evento									
>	10/02/25 12:26:03,000	1332016697.210000	CyEd9z3v2QM9aIBfbd	192.168.202.69	37012	192.168.28.253	22	undetermined	INBOUND SSH-2.0-OpenSSH_5.0	SSH-2.0-OpenSSH_4.5	- - - -
		host =	si-i-Of5d5a624a600293c-prd-p-3xn6m.splunkcloud.com	source =	ssh.log	sourcetype =	SSH:Pratica				
>	10/02/25 12:26:03,000	1332017793.040000	CrUTZx1hJvK1qFFT11	192.168.202.136	56815	192.168.21.203	22	failure	INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-
		host =	si-i-Of5d5a624a600293c-prd-p-3xn6m.splunkcloud.com	source =	ssh.log	sourcetype =	SSH:Pratica				
>	10/02/25 12:26:03,000	1332017778.370000	CZhG1136uZbVNG8uY1	192.168.202.136	56814	192.168.21.203	22	failure	INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-
		host =	si-i-Of5d5a624a600293c-prd-p-3xn6m.splunkcloud.com	source =	ssh.log	sourcetype =	SSH:Pratica				
>	10/02/25 12:26:03,000	1332017154.520000	C8XCE9WeJ5K5IEtPj	192.168.202.136	56802	192.168.21.203	22	undetermined	INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	
		host =	si-i-Of5d5a624a600293c-prd-p-3xn6m.splunkcloud.com	source =	ssh.log	sourcetype =	SSH:Pratica				
>	10/02/25 12:26:03,000	1332017111.420000	CB4eVG4sDCR1pFgRa	192.168.202.136	41186	192.168.27.203	22	failure	INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-
		host =	si-i-Of5d5a624a600293c-prd-p-3xn6m.splunkcloud.com	source =	ssh.log	sourcetype =	SSH:Pratica				
>	10/02/25 12:26:03,000	1332017807.510000	C0kT4dasAfZ4hp9i	192.168.202.136	41184	192.168.27.203	22	failure	INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-
		host =	si-i-Of5d5a624a600293c-prd-p-3xn6m.splunkcloud.com	source =	ssh.log	sourcetype =	SSH:Pratica				
>	10/02/25 12:26:03,000	1332017890.970000	CW0yQE1tr8Qkjj1S9	192.168.202.136	44979	192.168.23.203	22	failure	INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-
		host =	si-i-Of5d5a624a600293c-prd-p-3xn6m.splunkcloud.com	source =	ssh.log	sourcetype =	SSH:Pratica				
>	10/02/25 12:26:03,000	1332017864.540000	C6JLWj3NSX02Ee4PF1	192.168.202.136	44977	192.168.23.203	22	failure	INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-
		host =	si-i-Of5d5a624a600293c-prd-p-3xn6m.splunkcloud.com	source =	ssh.log	sourcetype =	SSH:Pratica				
>	10/02/25 12:26:03,000	1332016823.610000	CU6TCB38KBrCwLkFItd	192.168.202.136	51460	192.168.25.203	22	success	INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-
		host =	si-i-Of5d5a624a600293c-prd-p-3xn6m.splunkcloud.com	source =	ssh.log	sourcetype =	SSH:Pratica				

Posso quindi procedere con l'analisi, vado a filtrare la mia ricerca per i tentativi 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 tentativo di ripetuti tentativi di accesso sul servizio SSH.

Provo ad esaminare una riga per comprenderne meglio il significato.

10/02/25	1332014961.000000	C9Xd7r1rqMvxdE7h	192.168.202.136 56568	192.168.21.203	22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3
12:26:03,000	host = si-i-0f5d5a624a600293c.prd-p-3xn6m.splunkcloud.com index = main source = ssh.log sourcetype = SSH:Pratica								

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 connessione.
- **IP Destinataria** e porta con la quale si tenta di stabilire la connessione.
- **Failure**, indica il tentativo di connessione fallita.
- **INBOUND**, indica il tentativo di connessione in ingresso.
- **Nmap-ssh2**, indica che il client ha tentato la connessione mediante nmap.
- **SSH2.0 openSSH_5.8p1**, è la versione del servizio ssh sul server destinatario.

Vado ora a vedere le differenze rispetto al caso seguente.

10/02/25	133208493.580000	CuDIYeWdK5a9V0F32	192.168.202.138 49686	192.168.21.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.0	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3
12:26:03,000	host = si-i-0f5d5a624a600293c.prd-p-3xn6m.splunkcloud.com index = main source = ssh.log sourcetype = SSH:Pratica								

- **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.

10/02/25	1331903827.880000	CmsVqDHR180hT3eAj	192.168.202.68 38421	192.168.21.203	22	success	INBOUND	SSH-2.0-OpenSSH_5.0	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3
12:26:03,000	Azioni evento ▼								

In questo caso invece si nota come l'esito del tentativo 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
```

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

✓ 5.069 eventi (09/02/25 13:00:00,000 - 10/02/25 13:58:05,000) Nessun campionamento degli eventi ▼

Eventi Pattern Statistiche (1) Visualizzazione

Mostra: 20 per pagina ▼ / Formato ▼ ☒ Anteprima: on

count ↕

5069

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