

REPORT S10/L1

Analisi log

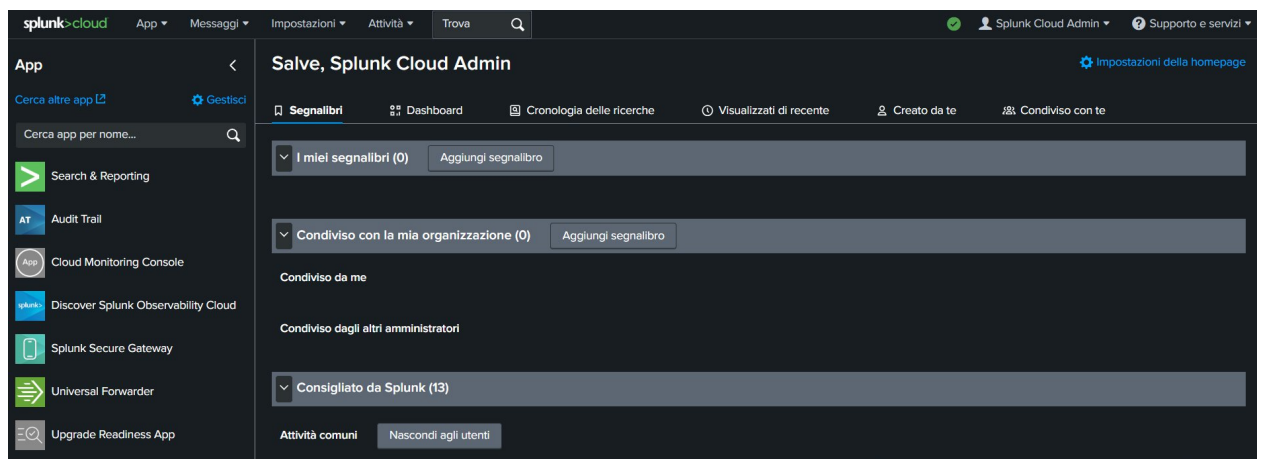
Traccia

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

Svolgimento

Per svolgere l'esercizio odierno ci colleghiamo al sito di Splunk e creiamo un nuovo account in modo da poter usare via cloud questo strumento di analisi dei log.

La pagina principale sarà questa:





E come prima cosa aggiungiamo nella sezione segnalibri un riferimento all'attività **“Aggiungi dati”**, poi lo apriamo e carichiamo il file che ci è stato dato durante la lezione.


Aprendo il link di *Aggiungi dati* verremmo reindirizzati a questa pagina:


Quali dati vuoi inviare alla piattaforma Splunk?

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

Dalla quale sceglieremo Carica, per importare il file ssh.log.

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 trascinandolo nella casella di destinazione qui di seguito. [Ulteriori informazioni](#)

File selezionato: **ssh.log**

Seleziona file

Ora premiamo su *Avanti*

Nelle sezioni successive lasciamo le impostazioni di default e andiamo Avanti:

Aggiungi dati

Selezione source **Imposta source type** Impostazioni di input Verifica Fine

< Indietro **Avanti >**

Imposta source type

Questa pagina consente di vedere come la piattaforma Splunk visualizza i dati prima dell'indicizzazione. Se gli eventi appaiono corretti e hanno i timestamp giusti, fare clic su "Avanti" per continuare. In caso contrario, utilizzare le opzioni di seguito per definire le suddivisioni in eventi e i timestamp corretti. Se non si è in grado di trovare un source type appropriato per i dati, crearne uno nuovo facendo clic su "Salva come".

Source: **ssh.log**

Source type: default **Salva come**

Formato: Mostra: 20 per pagina Visualizza: Elenco

	Ora	Evento
1	10/02/25 13:40:29.000	1331981011.840000 CTHco2B4R00PJYue 192.168.202.68 53633 192.168.28.254 22 failure INBOUND SSH-2.0-OpenSSH_5.0 SSH-1.99-Cisco-1.25
2	10/02/25 13:40:29.000	1331981030.210000 CBhpSz2Z13rdkxvvd 192.168.202.68 35820 192.168.23.254 22 failure INBOUND SSH-2.0-OpenSSH_5.0 SSH-1.99-Cisco-1.25
3	10/02/25 13:40:29.000	1331981032.030000 C2H6w259MT1Ak0B 192.168.202.68 36254 192.168.26.254 22 failure INBOUND SSH-2.0-OpenSSH_5.0 SSH-1.99-Cisco-1.25
4	10/02/25 13:40:29.000	1331981034.340000 Ce776r17XPbJ358yk0 192.168.202.68 37764 192.168.27.182 22 failure INBOUND SSH-2.0-OpenSSH_5.0 SSH-2.0-OpenSSH_5.0p1 Debian-tubuntu3

Ricerca
Analytics
Set di dati
Report
Allarmi
Dashboard
 Search & Reporting

Nuova ricerca

Salva come ▾
Crea vista tabella
Chiudi

7543 eventi (prima di 10/02/25 13:43:41,000) Nessun campionamento degli eventi ▾

Eventi (7543)
Pattern
Statistiche
Visualizzazione

Formato timeline ▾
Zoom indietro
+ Zoom area selezionata
x Deselezione
1 millisecondo per colonna

Formato ▾
Mostra: 20 per pagina ▾
Visualizza: Elenco ▾
< Prec 1 2 3 4 5 6 7 8 ... Avanti >

< Nascondi campi	Tutti i campi	Ora	Evento
CAMPI SELEZIONATI	host	10/02/25 13:43:28,000	1332816697.218900 CyDn3z3Q9waIbfnd 192.168.282.69 37812 192.168.28.253 22 undetermined INBOUND SSH-2.0-OpenSSH_5.0 SSH-2.0-OpenSSH_4.5 - - - -
	source sourcetype		host= sa-l02cb5e-908d7ed92.prd-p-8d0e8.splunkcloud.com source= ssh_log sourcetype= Mia
CAMPI INTERESSANTI	index	10/02/25 13:43:28,000	1332817753.848800 CrUTZx1njvLqFTFI 192.168.282.136 56815 192.168.21.283 22 failure INBOUND SSH-2.0-OpenSSH_5.3pl Debian-janubutu SSH-2.0-OpenSSH_5.3pl Debian-tubuntu - - - -
	indexname punct splunk_server timestamp		host= sa-l02cb5e-908d7ed92.prd-p-8d0e8.splunkcloud.com source= ssh_log sourcetype= Mia
		10/02/25 13:43:28,000	1332817778.378000 CZGt13ku2VNGduvU 192.168.282.136 56814 192.168.21.283 22 failure INBOUND SSH-2.0-OpenSSH_5.3pl Debian-janubutu SSH-2.0-OpenSSH_5.3pl Debian-tubuntu - - - -
			host= sa-l02cb5e-908d7ed92.prd-p-8d0e8.splunkcloud.com source= ssh_log sourcetype= Mia
		10/02/25 13:43:28,000	1332817154.528800 CBXOE9w3SKSIEtpj 192.168.282.136 56882 192.168.21.283 22 undetermined INBOUND SSH-2.0-OpenSSH_5.3pl Debian-janubutu SSH-2.0-OpenSSH_5.3pl Debian-tubuntu - - - -
			host= sa-l02cb5e-908d7ed92.prd-p-8d0e8.splunkcloud.com source= ssh_log sourcetype= Mia
+ Estrai nuovi campi		10/02/25 13:43:28,000	1332817111.428800 CB4wVG4sDCRfpfpa 192.168.282.136 41186 192.168.27.283 22 failure INBOUND SSH-2.0-OpenSSH_5.3pl Debian-janubutu SSH-2.0-OpenSSH_5.3pl Debian-tubuntu - - - -
			host= sa-l02cb5e-908d7ed92.prd-p-8d0e8.splunkcloud.com source= ssh_log sourcetype= Mia

Specificando la parola *failure* nella query (***source="ssh.log" failure***) possiamo analizzare nello specifico i log in cui vengono riportati i tentativi di connessione falliti. Vediamo un numero elevato di questi, provenienti da specifici indirizzi IP.

10/02/25 13:43:28,000	1332017793.040000 SH-2.0-OpenSSH_5.8p1 index = main	CrUTZx1hjVvk1qFFT11 Debian-1ubuntu3	-	-	-	-	192.168.202.136 56815	192.168.21.203 22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	S
10/02/25 13:43:28,000	1332017778.370000 SH-2.0-OpenSSH_5.8p1 index = main	CZhG1136uZbVNG8uY1 Debian-1ubuntu3	-	-	-	-	192.168.202.136 56814	192.168.21.203 22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	S
10/02/25 13:43:28,000	1332017111.420000 SH-2.0-OpenSSH_5.8p1 index = main	CB4eVG4sDCR1pFqRa Debian-1ubuntu3	-	-	-	-	192.168.202.136 41186	192.168.27.203 22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	S
10/02/25 13:43:28,000	1332017087.510000 SH-2.0-OpenSSH_5.8p1 index = main	COKT4dasAfZ4hxp9i Debian-1ubuntu3	-	-	-	-	192.168.202.136 41184	192.168.27.203 22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	S

10/02/25 13:43:28,000	1332014961.000000 penSSH_5.8p1 index = main	C9Xd7r1rqMvxxd7h Debian-1ubuntu3 -	-	192.168.202.136 56568	192.168.21.203 22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-0
10/02/25 13:43:28,000	1332014961.040000 penSSH_5.8p1 index = main	CHSj9guzUhPolkcA6 Debian-1ubuntu3 -	-	192.168.202.136 60076	192.168.21.102 22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-0
10/02/25 13:43:28,000	1332014960.620000 penSSH_5.8p1 index = main	C4wXMJ3QXd18LqZZc Debian-1ubuntu3 -	-	192.168.202.136 56543	192.168.21.203 22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-0

In particolare vediamo che :

- 192.168.202.141 ha effettuato ben 2365 tentativi falliti, un numero eccessivamente alto che suggerisce un attacco brute-force mirato.
- Gli altri IP (192.168.202.110, 192.168.204.45, 192.168.202.140, 192.168.202.68) mostrano anch'essi un numero significativo di tentativi di connessione falliti, indicando attività sospette.

Un altro aspetto critico della sicurezza sta nelle versioni di SSH identificate. L'uso di versioni obsolete o vulnerabili di SSH può facilitare i vari tipi di attacchi. In particolare vediamo che le versioni installate sono obsolete, pertanto esposte ad attacchi sia brute force che man-in-the-middle.

Ad esempio:

1. SSH-1.99-Cisco-1.25 & SSH-1.99-OpenSSH_4.5:
 - Supportano SSH-1, completamente insicuro e può essere attaccato con sniffing delle credenziali. (Attacchi possibili: man-in-the-middle (MITM), downgrade attack).
2. OpenSSH 5.8p1 (Debian 7ubuntu1 & 1ubuntu3):
 - Rischio di bypassare l'autenticazione (Attacchi possibili: Privilege Escalation, Attacco Brute-Force Facilitato).
3. OpenSSH 4.5:
 - Versione molto vecchia che permette attacchi di tipo MITM.