


Esercizio S10/L1


Esercizio di oggi: Analisi log


Analizzare il log **ssh.log** fornito e indicare elementi rilevanti, ovvero login falliti, tentativi di attacco ecc. Non sono interessato ai login di successo. Trovare tutto ciò che è anomalo.


Importazione File

Una volta scaricato il file **ssh log**, importiamolo e seguiamo i passi da seguire indicati da Splunk

**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

Importazione File

Aggiungi dati



< Indietro

Avanti >

Seleziona 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

Trascina i file di dati qui

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



File caricato con successo.

Analisi







Aggiungi dati

< Indietro

Avanti >

rma Splunk visualizza i dati prima dell'indicizzazione. Se gli eventi appaiono corretti e hanno i
: In caso contrario, utilizzare le opzioni di seguito per definire le suddivisioni in eventi e i
n source type appropriato per i dati, crearne uno nuovo facendo clic su "Salva come".

Visualizza sintesi degli eventi


Salva come	Formato ▼		Mostra: 20 per pagina ▼		Visualizza: Elenco ▼		< Prec 1 2 3 4 5 6 7 8 ... Avanti >									
		Ora	Evento													
	1		10/02/25 11:51:46,000	1331901011.840000	CTHcOo3BARDOPDjYue	192.168.202.68	53633	192.168.28.254	22	failure	INBOUND	SSH-2.0-0				
	penSSH_5.0 SSH-1.99-Cisco-1.25 - - - -															
	timestamp = none															
	2		10/02/25 11:51:46,000	1331901030.210000	CBHpSz2Zi3rdKbAvwd	192.168.202.68	35820	192.168.23.254	22	failure	INBOUND	SSH-2.0-0				
	penSSH_5.0 SSH-1.99-Cisco-1.25 - - - -															
timestamp = none																
3		10/02/25 11:51:46,000	1331901032.030000	C2h6wz2S5MWTiAk6Hb	192.168.202.68	36254	192.168.26.254	22	failure	INBOUND	SSH-2.0-0					
penSSH_5.0 SSH-1.99-Cisco-1.25 - - - -																
timestamp = none																
4		10/02/25 11:51:46,000	1331901034.340000	CeY76r1JXPbjJS8yKb	192.168.202.68	37764	192.168.27.102	22	failure	INBOUND	SSH-2.0-0					
penSSH_5.0 SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - -																
timestamp = none																
5		10/02/25 11:51:46,000	1331901041.920000	CPJHML3uGn4IV2MGWi	192.168.202.68	40244	192.168.27.101	22	failure	INBOUND	SSH-2.0-0					
penSSH_5.0 SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1 - - - -																
timestamp = none																
6		10/02/25 11:51:46,000	1331901079.500000	CENo31KCFmQXZ00k	192.168.202.68	36127	192.168.27.202	22	failure	INBOUND	SSH-2.0-0					
penSSH_5.0 SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - -																
timestamp = none																



Analisi

Messaggi ▾

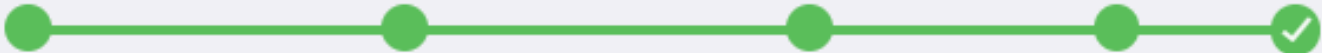
Impostazioni ▾

Attività ▾

Trova 

  Splunk Cloud Admin ▾

Aggiungi dati




Seleziona source

Imposta source type


Impostazioni di input

Verifica

Fine 

< Indietro


Avanti >




File è stato caricato correttamente.

Configurare gli input da Impostazioni > [Input dati](#)


Avvia ricerca

Eseguire una ricerca tra i dati ora oppure visualizzare [esempi ed esercitazioni](#). 


Estrai campi

Creare estrazioni di campi search-time. [Ulteriori informazioni sui campi](#). 


Aggiungi altri dati

Aggiungere altri input di dati ora oppure visualizzare [esempi ed esercitazioni](#). 

Scarica app

Le app consentono di fare di più con i propri dati. [Ulteriori informazioni](#). 

Crea dashboard

Visualizza le ricerche. [Ulteriori informazioni](#). 

Analisi

Il file presenta numerosi tentativi falliti di accesso al servizio SSH sulla porta 22, gli attacchi partono da host diversi e raggiungono altrettanti host diversi

Nuova ricerca

Salva come ▾Crea vista tabellaChiudi

index="main" sourcetype="Scansione"

Sempre ▾

Q

✓ 7.143 eventi (prima di 10/02/25 14:56:32,000) Nessun campionamento degli eventi ▾

Processo ▾

||→→🖨️⬇️

 Gruppo basato sui criteri ▾ ? Modalità intelligente ▾

Eventi (7.143)PatternStatisticheVisualizzazione

🔧 Formato timeline ▾

— Zoom indietro

+ Zoom area selezionata

✕ Deseleziona

1 millisecondo per colonna

🔧 Formato ▾Mostra: 50 per pagina ▾Visualizza: Elenco ▾

< Prec

12345678...Avanti >

< Nascondi campi

☰ Tutti i campi

CAMPI SELEZIONATI

a host 1

a index 1

a punct 19

a source 1

a sourcetype 1

CAMPI INTERESSANTI

linecount 1

a splunk_server 1

a timestamp 1

+ Estrai nuovi campi

i	Ora	Evento
>	10/02/25 13:09:42,000	1332016697.210000 CyEd9z3v2QM9aIBfbd 192.168.202.69 37012 192.168.28.253 22 undetermined INBOUND SSH-2.0-OpenSSH_5.0 SSH-2.0-0 penSSH_4.5 - - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt-.-.-t-t-t-t-t- source = ssh.log sourcetype = Scansione
>	10/02/25 13:09:42,000	1332017793.040000 CrUTZx1hjVk1qFFT11 192.168.202.136 56815 192.168.21.203 22 failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7 S SH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt-.-.-t-.-t-t-t-t-t- source = ssh.log sourcetype = Scansione
>	10/02/25 13:09:42,000	1332017778.370000 CZhG1136uZbVNG8uY1 192.168.202.136 56814 192.168.21.203 22 failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7 S SH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt-.-.-t-.-t-t-t-t-t- source = ssh.log sourcetype = Scansione
>	10/02/25 13:09:42,000	1332017154.520000 C0X0E9Wej5K5IETpj 192.168.202.136 56802 192.168.21.203 22 undetermined INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubu ntu7 SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt-.-.-t-.-t-t-t-t-t- source = ssh.log sourcetype = Scansione
>	10/02/25 13:09:42,000	1332017111.420000 CB4eVG4sDCR1pFqRa 192.168.202.136 41186 192.168.27.203 22 failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7 S SH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt-.-.-t-.-t-t-t-t-t- source = ssh.log sourcetype = Scansione

Analisi

Da quello che vediamo i log riguardanti il servizio SSH hanno lasciato delle “tracce”, indicando che quello che i vari host attaccanti stanno facendo è una scansione **nmap** alla ricerca di una vulnerabilità su tale servizio

Nuova ricerca

Salva come ▾Crea vista tabellaChiudi

"SSH-1.5-Nmap-SSH1-Hostkey"Sempre ▾

✓ 251 eventi (prima di 10/02/25 15:04:10,000)Nessun campionamento degli eventi ▾Processo ▾Gruppo basato sui criteri ▾? Modalità intelligente ▾

Eventi (251)PatternStatisticheVisualizzazione

Formato timeline ▾ Zoom indietro Zoom area selezionata Deseleziona1 millisecondo per colonna

< Nascondi campi

Tutti i campi

CAMPI SELEZIONATI

a host 1

a index 1

a punct 4

a source 1

a sourcetype 1

CAMPI INTERESSANTI

linecount 1

a splunk_server 1

a timestamp 1

+ Estrai nuovi campi

i	Ora	Evento
>	10/02/25 13:09:42,000	1332014961.950000 CkzM6a2xKKIkrWRGv4 192.168.202.136 48869 192.168.21.253 22 undetermined INBOUND SSH-1.5-Nmap-SSH1-Hostkey S SH-1.99-OpenSSH_4.5 - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt---t-.-t-t-t-t-t- source = ssh.log sourcetype = Scansione
>	10/02/25 13:09:42,000	1332014960.260000 CfSqT13pB1V35QL4P1 192.168.202.136 56523 192.168.21.203 22 undetermined INBOUND SSH-1.5-Nmap-SSH1-Hostkey S SH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt---t-.-_t-t-t-t-t- source = ssh.log sourcetype = Scansione
>	10/02/25 13:09:42,000	1332014960.250000 CaeoRv2zEj5ctI842i 192.168.202.136 60023 192.168.21.102 22 undetermined INBOUND SSH-1.5-Nmap-SSH1-Hostkey S SH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt---t-.-_t-t-t-t-t- source = ssh.log sourcetype = Scansione
>	10/02/25 13:09:42,000	1332013311.940000 CzCQhG2wwSON6CwSVh 192.168.202.141 5730 192.168.229.101 22 undetermined INBOUND SSH-1.5-Nmap-SSH1-Hostkey S SH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1 - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt---t-.-_t-t-t-t-t- source = ssh.log sourcetype = Scansione

Analisi

punct



19 Valori, 100% di eventi

Selezionato

Sì

No

Report

Primi valori

Primi valori nel tempo

Valori rari

Eventi con questo campo

Primi 10 valori	Conteggio	%	
.tt...tt...tttt-t-.-._-t-t-t-t-t-	2.799	39,185%	<div></div>
.tt...tt...tttt-.-.t-.-._-t-t-t-t-t-	1.527	21,378%	<div></div>
.tt...tt...tttt-.-.t-.-.t-t-t-t-t-	646	9,044%	<div></div>
.tt...tt...tttt-.-.-t-.-._-t-t-t-t-t-	385	5,39%	<div></div>
.tt...tt...tttt-.-.t-.-.t-t-t-t-t-	298	4,172%	<div></div>
.tt...tt...tttt-.-._-t-.-._-t-t-t-t-t-	292	4,088%	<div></div>
.tt...tt...tttt-.-._-t-.-.t-t-t-t-t-	247	3,458%	<div></div>
.tt...tt...tttt-.-._-t-.-.t-t-t-t-t-	216	3,024%	<div></div>
.tt...tt...tttt-.-.-t-.-.t-t-t-t-t-	206	2,884%	<div></div>
.tt...tt...tttt-t-.-.t-t-t-t-t-	172	2,408%	<div></div>

Se c'è una cosa che riusciamo a notare è il campo **punct**, esso è una rappresentazione della struttura di punteggiatura di un evento, che aiuta a identificare pattern nei log ignorando lettere e numeri. Come vediamo ce ne sono 19 in totale, di cui 2 rappresentano la maggior parte degli attacchi.

Analisi

RicercaAnalyticsSet di datiReportAllarmiDashboard

>

Search & Reporting

Nuova ricerca

Salva comeCrea vista tabellaChiudi

index="main" sourcetype="Scansione" punct=".tt...tt...tttt-.t-.-._-t-t-t-t-t-

Sempre

Q

✓ 1.527 eventi (prima di 10/02/25 14:38:23,000)

Nessun campionamento degli eventi

Processo

||■↶↷🖨️⬇️

Gruppo basato sui criteri

! Modalità intelligente

Eventi (1.527)

Pattern

Statistiche

Visualizzazione

🔧 Formato timeline

— Zoom indietro

+ Zoom area selezionata

× Deseleziona

1 millisecondo per colonna

🔧 FormatoMostra: 50 per paginaVisualizza: Elenco

< Prec12345678...Avanti >

< Nascondi campi

Tutti i campi

CAMPI SELEZIONATI

a host 1

a index 1

a punct 1

a source 1

a sourcetype 1

CAMPI INTERESSANTI

linecount 1

a splunk_server 1

a timestamp 1

+ Estrai nuovi campi

i	Ora	Evento
>	10/02/25 13:09:42,000	1332016697.140000 C1DGv73pPwLrLznhk 192.168.202.69 36782 192.168.26.203 22 failure INBOUND SSH-2.0-OpenSSH_5.0 SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt-.t-.-._-t-t-t-t-t- source = ssh.log sourcetype = Scansione
>	10/02/25 13:09:42,000	1332014962.120000 CvGvWX2pW7tRDE45p1 192.168.202.136 56642 192.168.21.203 22 undetermined INBOUND SSH-1.5-NmapNSE_1.0 SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt-.t-.-._-t-t-t-t-t- source = ssh.log sourcetype = Scansione
>	10/02/25 13:09:42,000	1332014961.450000 C1dN9xRjGsLuup936 192.168.202.136 60105 192.168.21.102 22 undetermined INBOUND SSH-1.5-NmapNSE_1.0 SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt-.t-.-._-t-t-t-t-t- source = ssh.log sourcetype = Scansione
>	10/02/25 13:09:42,000	1332013311.930000 CLJ1Ay26WC9gnbJkb7 192.168.202.141 5732 192.168.229.101 22 undetermined INBOUND SSH-1.5-NmapNSE_1.0 SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1 - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt-.t-.-._-t-t-t-t-t- source = ssh.log sourcetype = Scansione

Analisi

Infine, vediamo che ci sono 301 log di successo, talvolta provenienti dagli stessi IP che hanno effettuato le scansioni. Quindi è logico dedurre che l'attaccante sia riuscito a trovare delle credenziali di accesso.

Nuova ricerca

Salva come ▾Crea vista tabellaChiudi

index="main" sourcetype="Scansione" success

Sempre ▾

✓ 301 eventi (prima di 10/02/25 15:20:50,000)Nessun campionamento degli eventi ▾

Processo ▾

Process icons

Gruppo basato sui criteri ▾Modalità intelligente ▾

Eventi (301)PatternStatisticheVisualizzazione

Formato timeline ▾Zoom indietroZoom area selezionataDeseleziona

1 millisecondo per colonna

Formato ▾Mostra: 50 per pagina ▾Visualizza: Elenco ▾

< Prec

1234567

Avanti >

< Nascondi campiTutti i campi

CAMPI SELEZIONATI

a host 1

a index 1

a punct 8

a source 1

a sourcetype 1

CAMPI INTERESSANTI

linecount 1

a splunk_server 1

a timestamp 1

+ Estrai nuovi campi

i	Ora	Evento
>	10/02/25 13:09:42,000	1332016823.610000 CU6TCB38KBrCWLkfId 192.168.202.136 51460 192.168.25.203 22 success INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7 S SH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt-.-_t-.-t-t-t-t-t- source = ssh.log sourcetype = Scansione
>	10/02/25 13:09:42,000	1332016462.720000 CCWY6r6aIU46DQbA6 192.168.202.136 54411 192.168.27.253 22 success INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7 S SH-2.0-OpenSSH_4.5 - - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt-.-_t-.-t-t-t-t-t- source = ssh.log sourcetype = Scansione
>	10/02/25 13:09:42,000	1332016153.430000 CFMSdSFnEph3uY0o9 192.168.202.136 54405 192.168.27.253 22 success INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7 S SH-2.0-OpenSSH_4.5 - - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt-.-_t-.-t-t-t-t-t- source = ssh.log sourcetype = Scansione
>	10/02/25 13:09:42,000	1332014219.680000 Ck402qt1aBBTEkgF6 192.168.202.76 52321 192.168.26.254 22 success INBOUND SSH-2.0-PuTTY_Release_0.60 SSH-1.99- Cisco-1.25 - - - - - host = si-i-01e92308449c65881.prd-p-by1b3.splunkcloud.com index = main punct = .tt...tt...tttt-.-t-.-t-t-t-t-t- source = ssh.log sourcetype = Scansione