

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

Ricerca | Splunk 9.4.0

127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"ssh.log"%20host%3D"DESKTOP-OB98A0T"&earliest=0&latest=&sid=1739192424.67&display.pag...

Ricerca Analytics Set di dati Report Allarmi Dashboard Search & Reporting

Nuova ricerca

source="ssh.log" host="DESKTOP-OB98A0T"

✓ 14.286 eventi (prima di 10/02/25 14:00:25,000) Nessun campionamento degli eventi

Processo Zoom indietro Zoom area selezionata Deseleziona 1 minuto per colonna

Eventi (14.286) Pattern Statistiche Visualizzazione

Formato timeline Zoom indietro Zoom area selezionata Deseleziona 1 minuto per colonna

Formato Mostra: 20 per pagina Visualizza: Elenco

	i	Ora	Evento
>	10/02/25 14:00:21,000	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 = DESKTOP-OB98A0T source = ssh.log sourcetype = default
>	10/02/25 14:00:21,000	1332017793.040000	CrUTZx1h3VklqFFT11 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 = DESKTOP-OB98A0T source = ssh.log sourcetype = default
>	10/02/25 14:00:21,000	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 = DESKTOP-OB98A0T source = ssh.log sourcetype = default

CAMPI SELEZIONATI
a host 1
a source 1
a sourcetype 1

CAMPI INTERESSANTI
a index 1
linecount 1
a punct 19
a splunk_server 1

Ricerca | Splunk 9.4.0

127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"ssh.log"%20host%3D"DESKTOP-OB98A0T"&earliest=0&latest=&sid=1739192424.67&display.pag...

Formato Mostra: 20 per pagina Visualizza: Elenco

	i	Ora	Evento
>	10/02/25 14:00:21,000	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 = DESKTOP-OB98A0T source = ssh.log sourcetype = default
▼	10/02/25 14:00:21,000	1332017793.040000	CrUTZx1h3VklqFFT11 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
>	10/02/25 14:00:21,000	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 = DESKTOP-OB98A0T source = ssh.log sourcetype = default
>	10/02/25 14:00:21,000	1332017154.520000	C0X0E9Wej5K5IEtpj 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 = DESKTOP-OB98A0T source = ssh.log sourcetype = default

Azioni evento ▼

Tipo	Campo	Valore	Azioni
Selezionato	host ▼	DESKTOP-OB98A0T	▼
	source ▼	ssh.log	▼
	sourcetype ▼	default	▼
Evento	timestamp ▼	none	▼
Ora	_time ▼	2025-02-10T14:00:21.000+01:00	▼
Default	index ▼	main	▼
	linecount ▼	1	▼
	punct ▼	.tt...tt...tttt-...-t-...-t-t-t-t-	▼
	splunk_server ▼	DESKTOP-OB98A0T	▼