Report Esercizio 10/02/2025

Analisi Log Splunk Leonardo Catalano

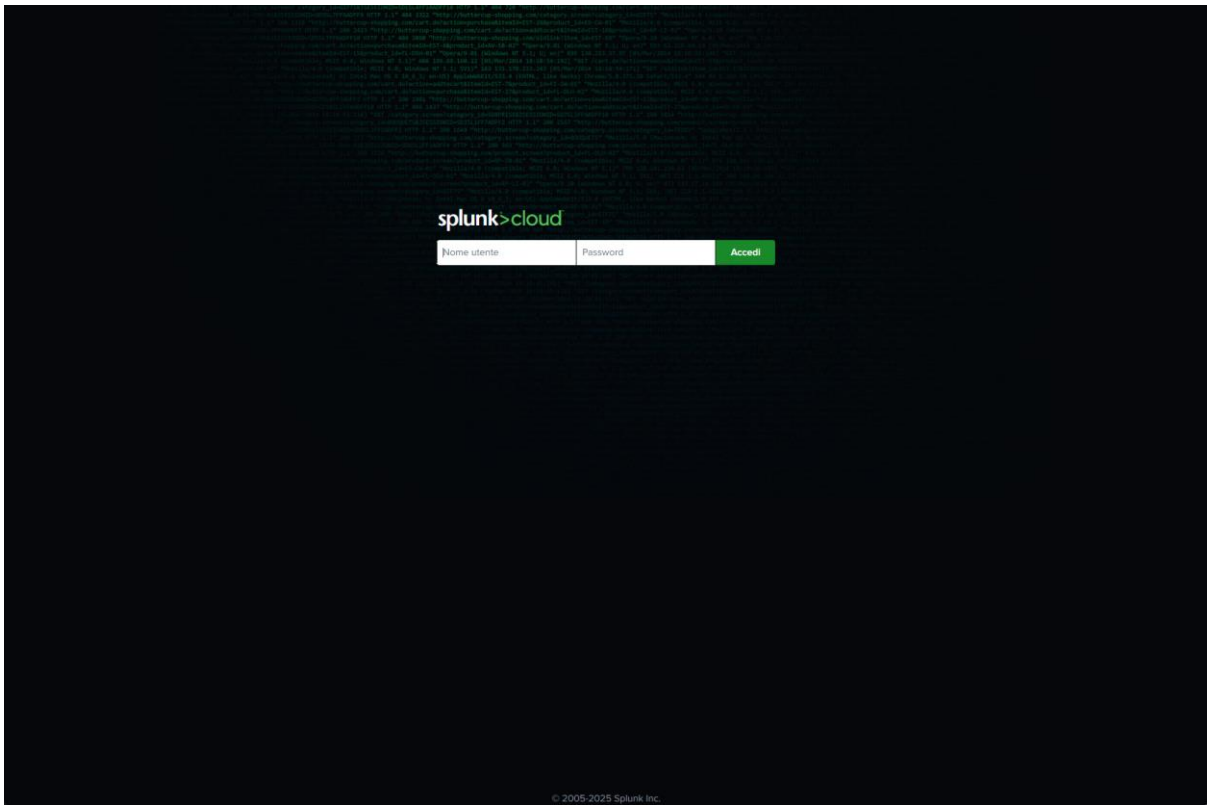
“La traccia di oggi ci chiede di effettuare un’analisi con Splunk di un log “ssh.log.”

Le fasi da effettuare saranno le seguenti:

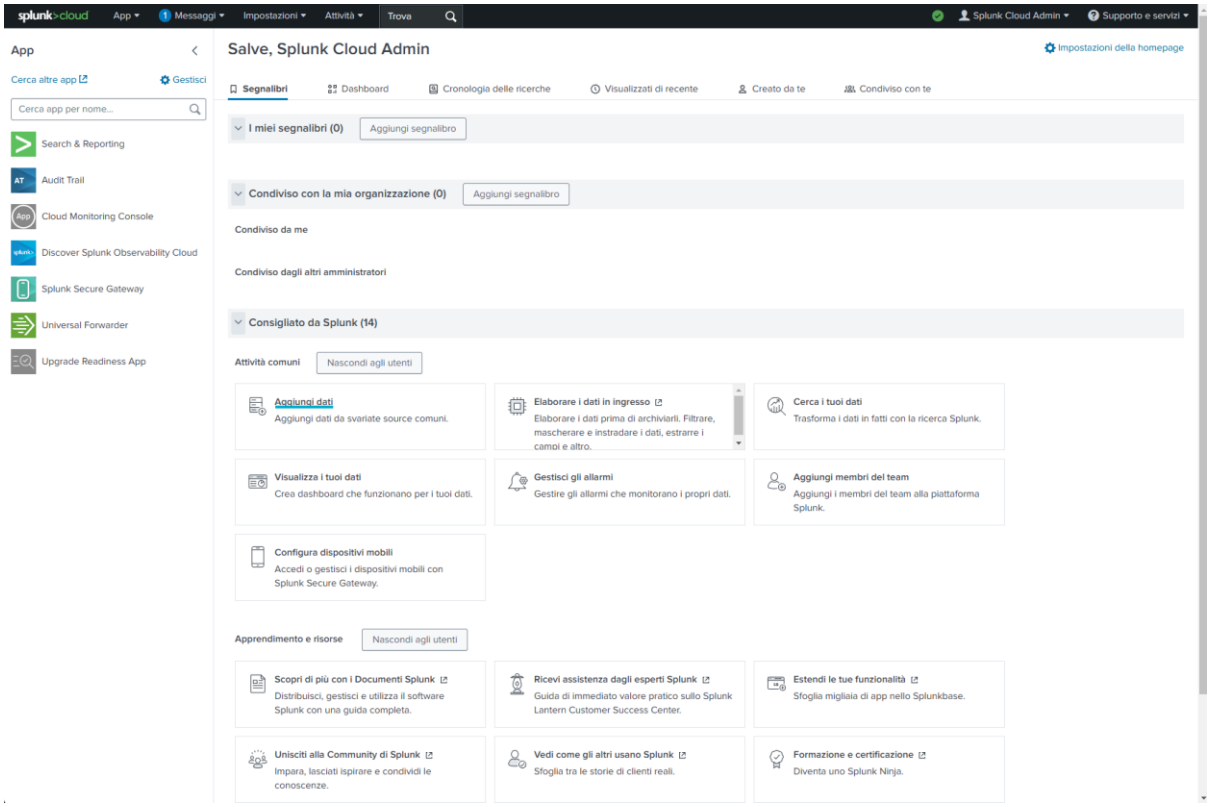
1. Identificare ed analizzare gli elementi rilevanti, (ovvero login falliti, tentativi di attacco, traffico anomalo).

-Splunk CloudMacchina Kali Linux:

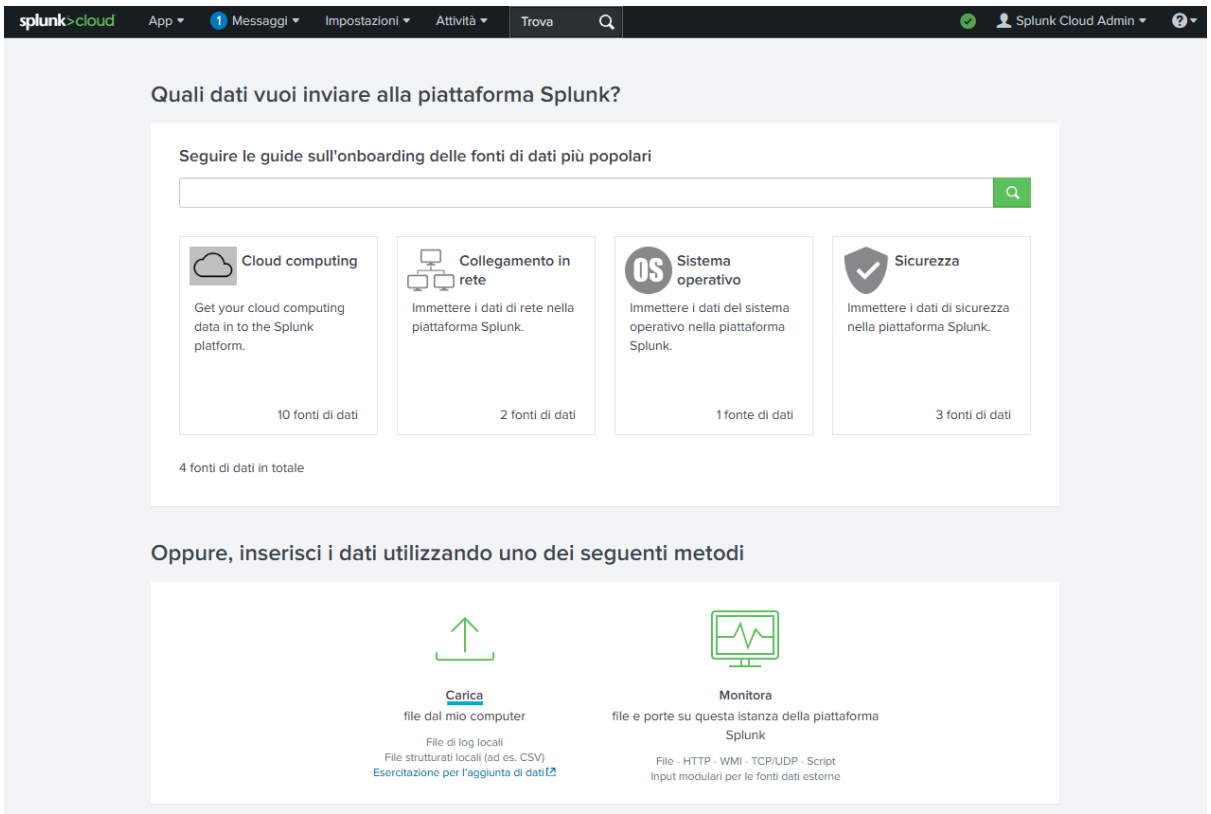
Per poter effettuare l’analisi con Splunk, in questo caso utilizzo Splunk Cloud.
Per poter utilizzare Splunk Cloud dovremo registrarsi sul sito e utilizzare le credenziali ricevute per accedere alla nostra interfaccia privata di Splunk Cloud.

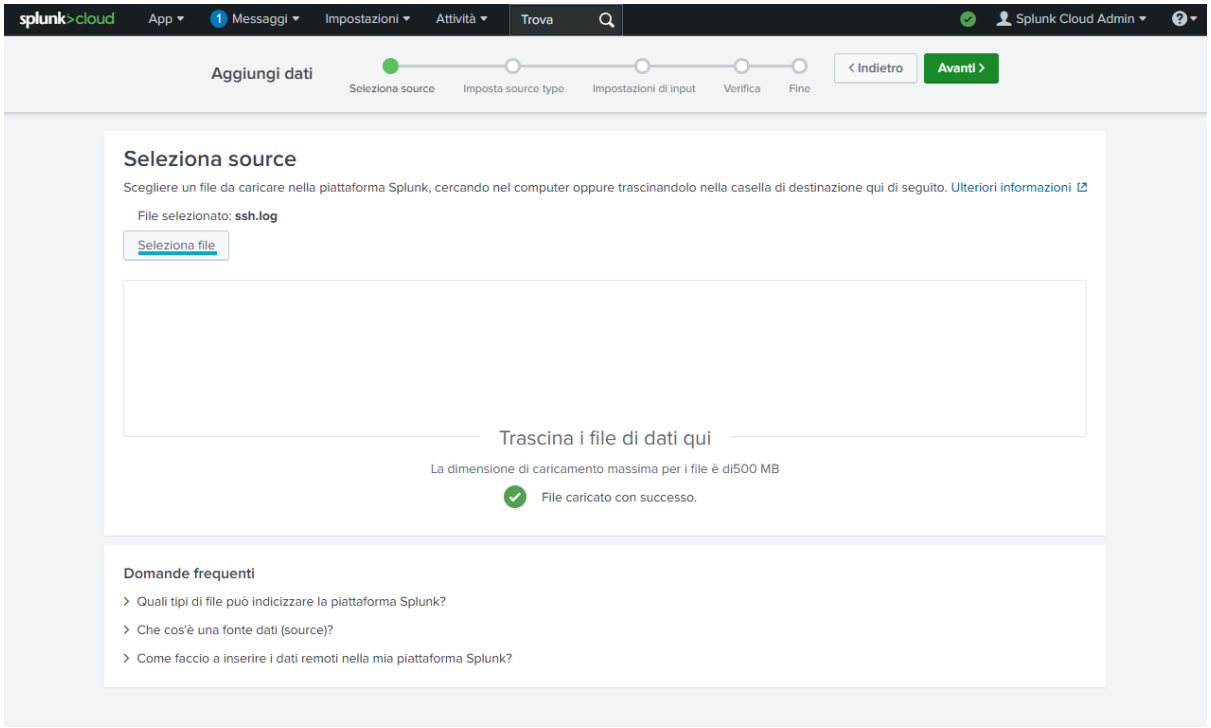


Una volta inserito i dati di login avremo la nostra interfaccia privata di Splunk Cloud.

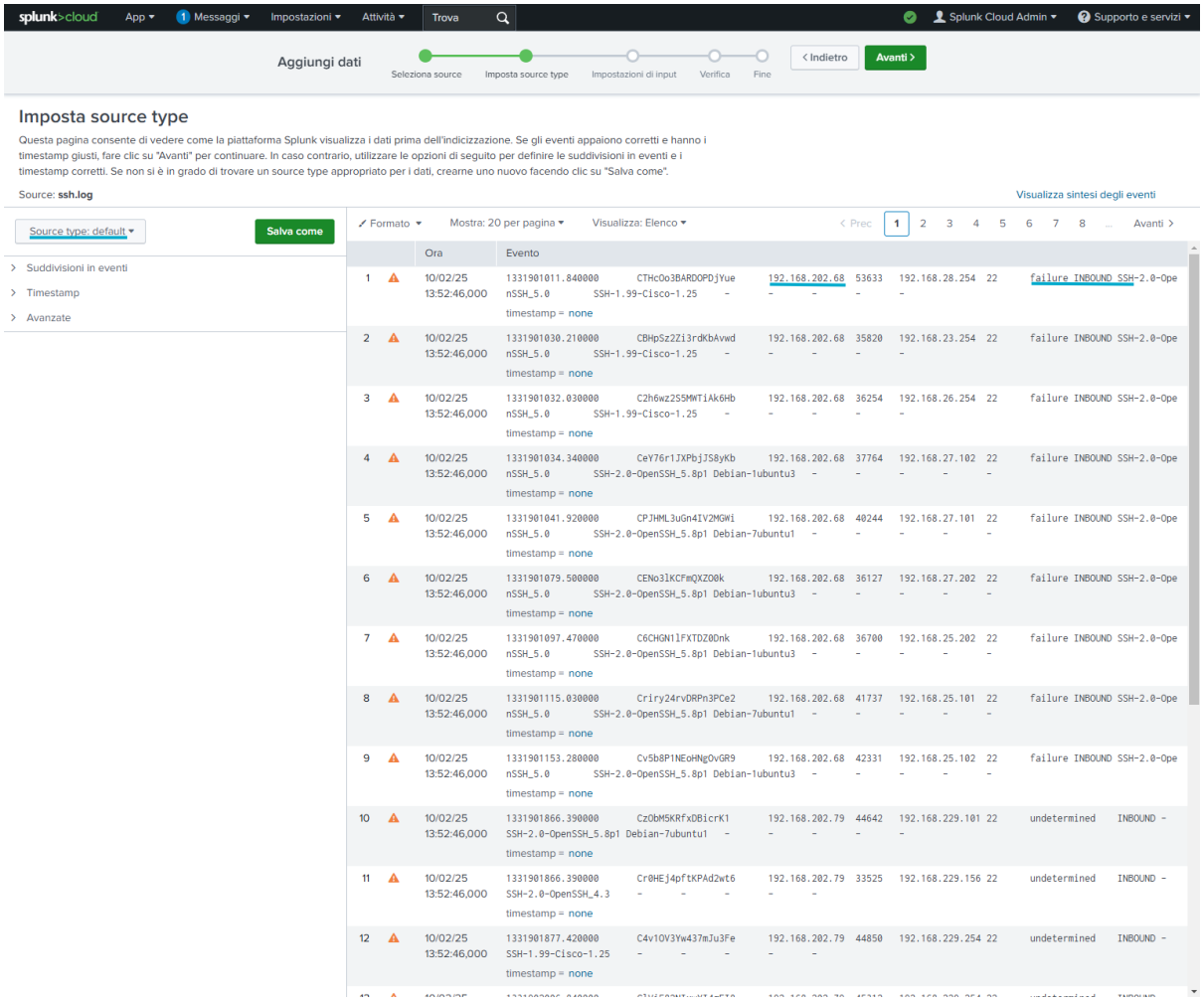


Andando nella sezione Aggiungi dati possiamo uploudare il file ”ssh.log”.



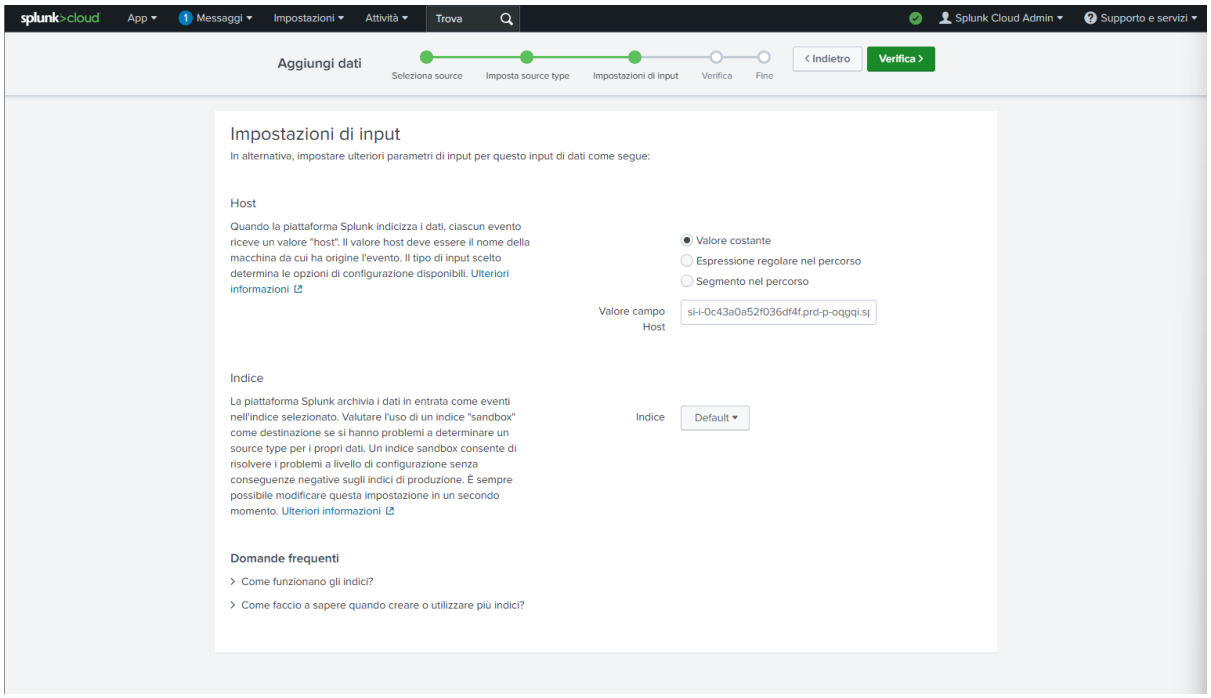


Da selezione file scegliamo il file da uploudare ”ssh.log” e andiamo avanti.

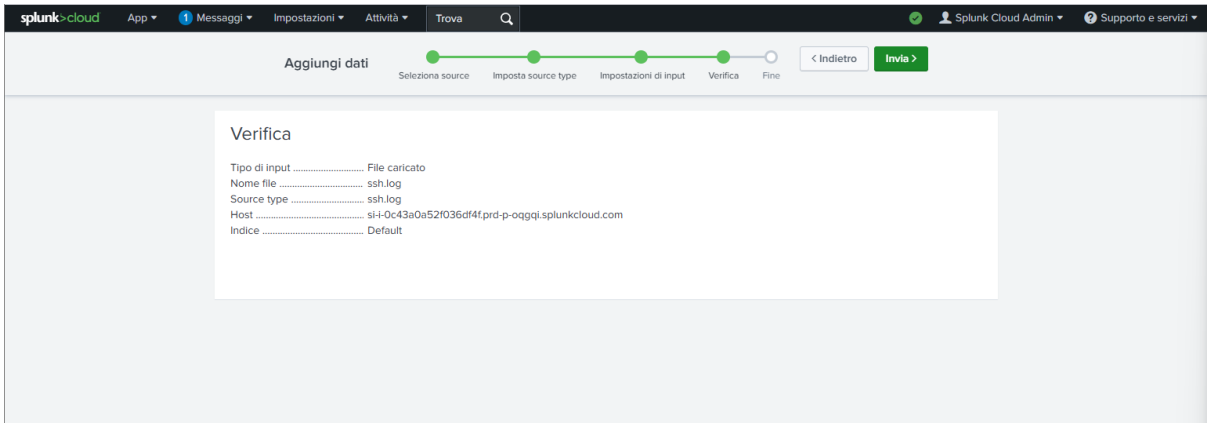


Ora dovremo impostare il source Type, per permettere a Splunk di visualizzare in

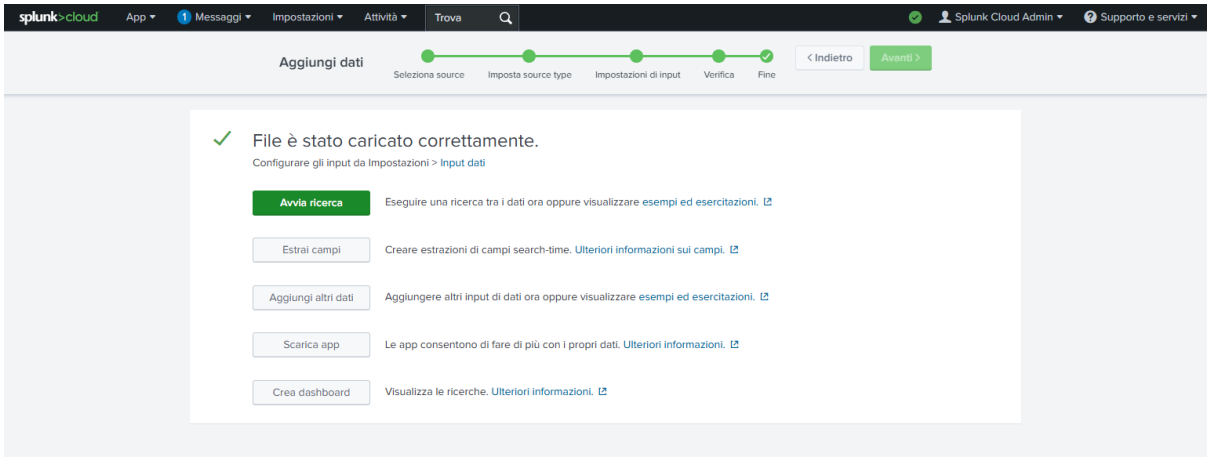
maniera corretta i dati, lasciando quello di default si può vedere che cmq va bene e ci sono i primi log di tentativi falliti di login ”failure INBOUND SSH” da parte dell’indirizzo 192.168.202.68.
Andando avanti andremo ad impostare i parametri di input.



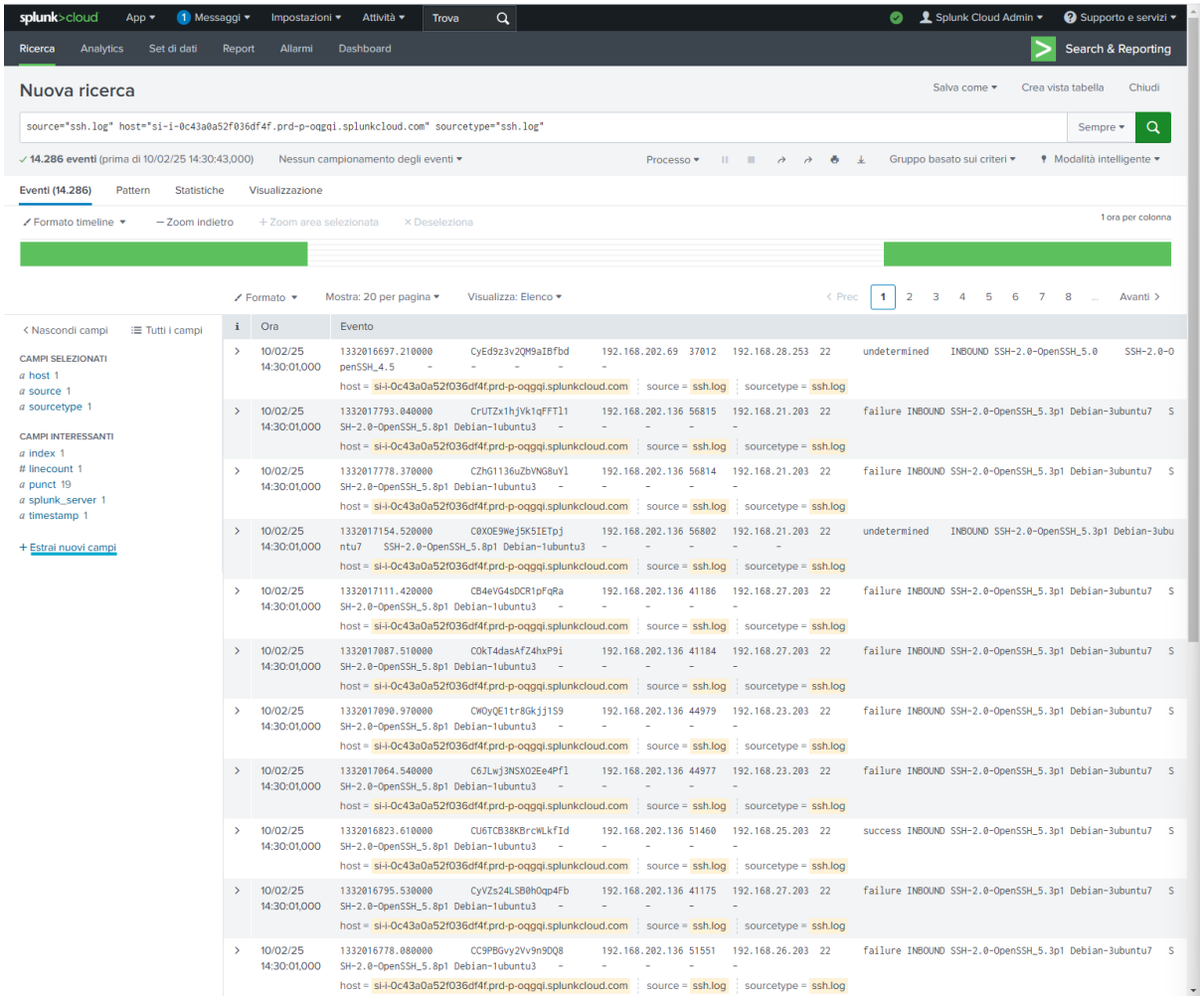
In questo caso lascio i parametri di Default e vado su ”Verifica”.



Invio il file e le impostazioni:

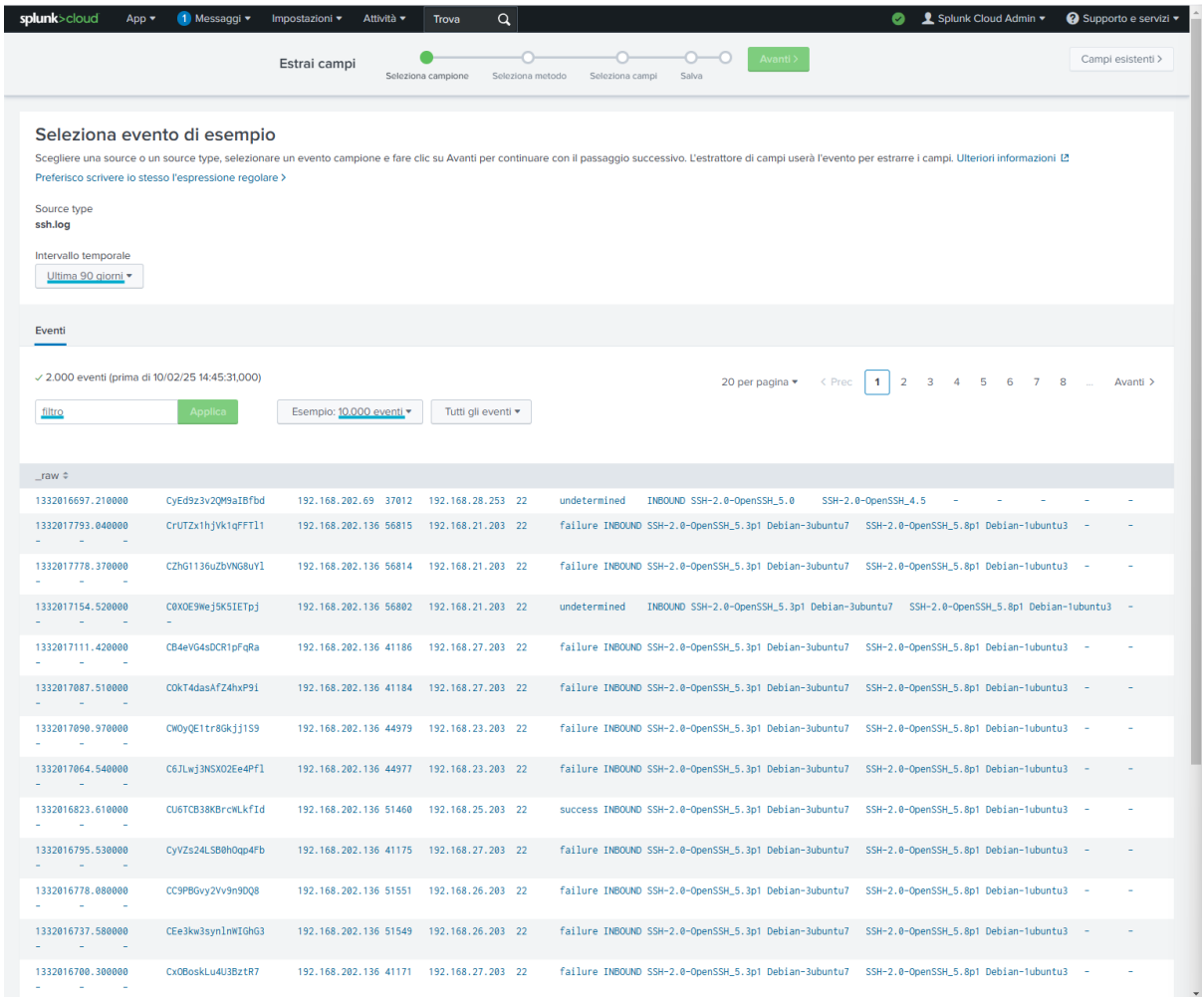


Da cui possiamo avviare la ricerca, ed estrarre i campi interessati con le query:



Questa è l'interfaccia finale, da cui possiamo modificare la query e i filtri per andare a ricercare soltanto dei determinati log.

Se andiamo su Estrai nuovi campi, ci si aprirà un'interfaccia dove potremmo andare ad applicare dei filtri sui log .



Settando il tempo sugli ultimi 90 giorni, come numero eventi 10.000 e su ”filtro” possiamo andare a scrivere il filtro che vogliamo, il 1* controllo che faccio è sui failure per vedere quanti sono.

-Filtro Failure:

✓ 1.960 eventi (prima di 10/02/25 14:50:25,000)

20 per pagina ▾ ‹ Prec **1** 2 3 4 5 6 7 8 … Avanti ›

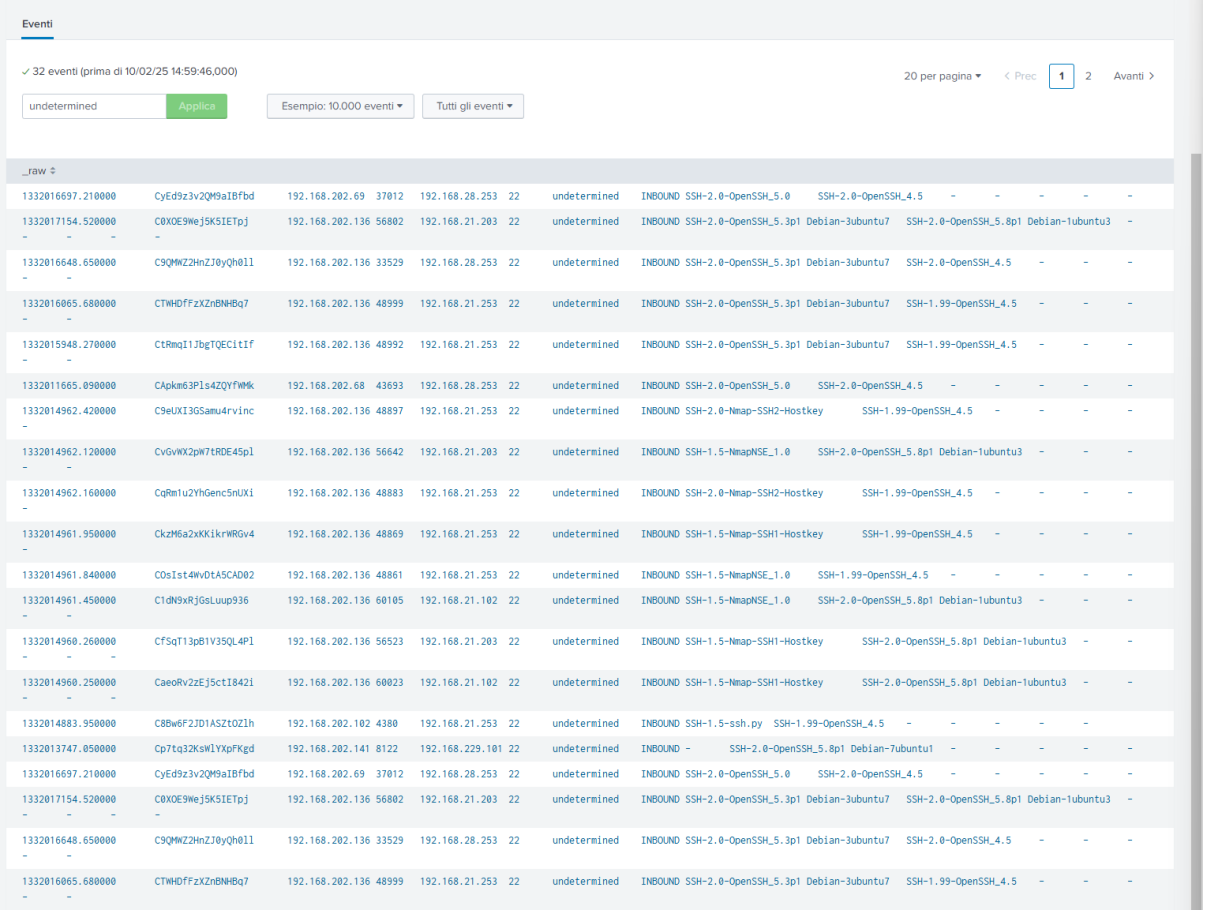
failure | Applica | Esempio: 10.000 eventi ▾ | Tutti gli eventi ▾

_raw ⇕

1332017793.040000	CrUTZx1hjVk1qFFTl1	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	-	-	-	-	-
1332017778.370000	CZhG1136uZbVNG8uYl	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	-	-	-	-	-
1332017111.420000	CB4eVG4sDCR1pFqRa	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	-	-	-	-	-
1332017087.510000	COkT4dasAfZ4hxP9i	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	-	-	-	-	-
1332017090.970000	CWOyQE1tr8Gkjj1S9	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	-	-	-	-	-
1332017064.540000	C6JLwj3NSXO2Ee4Pfl	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	-	-	-	-	-
1332016795.530000	CyVZs24LSB0hOqp4Fb	192.168.202.136	41175	192.168.27.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-
1332016778.080000	CC9PBGvy2Vv9n9DQ8	192.168.202.136	51551	192.168.26.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-
1332016737.580000	CEe3kw3synlnWIGhG3	192.168.202.136	51549	192.168.26.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-
1332016700.300000	CxOBoskLu4U3BztR7	192.168.202.136	41171	192.168.27.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-
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	-	-	-	-	-
1332016117.960000	Cs98WG3OoUF4oJU3Cc	192.168.202.136	43815	192.168.25.253	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_4.5	-	-	-	-	-
1332016093.390000	CQ3yf24THfNo9TJIH4	192.168.202.136	49316	192.168.24.253	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_4.5	-	-	-	-	-
1332016069.920000	CDPaSrARYJJjkK1N8	192.168.202.136	49314	192.168.24.253	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_4.5	-	-	-	-	-
1332015982.680000	ChRr9H38HOxtOmJO23	192.168.202.136	33059	192.168.23.253	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_4.5	-	-	-	-	-
1332015954.440000	CP5R321S3mjV7UEGv8	192.168.202.136	33057	192.168.23.253	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_4.5	-	-	-	-	-
1332015936.780000	CHqI5M2OCvO9wOJwAh	192.168.202.136	60265	192.168.21.102	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-
1332014961.000000	C9Xd7rlrqMvvxdE7h	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	-	-	-	-	-
1332014961.040000	ChSj9guzUhPolkcA6	192.168.202.136	60076	192.168.21.102	22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-
1332014960.620000	C4wXMJ3QXd18LqQZZc	192.168.202.136	56543	192.168.21.203	22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-

Analizzando i tentativi falliti di Inbound con L’SSH al Web Server Debian, noto che c’è un attaccante che fa parte della rete 192.168.21.0 che con vari indirizzi ip sta attaccando varie macchine con diversi indirizzi ip anche di reti diversi (come sottolineati) per cercare di accedere con l’ssh ai web server.
Ciò mi fa pensare ad un attacco di brute force.

-Filtro Undetermined:
Oltre ai tipi failure ho trovato il tipo undetermined (indeterminati) e anche qui trovo tentativi di accesso “falliti” ma anche degli Nmap sugli host.



Eventi

✓ 32 eventi (prima di 10/02/25 14:59:46,000)

20 per pagina ‹ Prec 1 2 Avanti ›

undetermined Applica Esempio: 10.000 eventi Tutti gli eventi

_raw														
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	-	-	-	-	-
1332017154.520000	C0XOE9Wej5K5IETpj	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	-	-	-	-	-
1332016648.650000	C9QMWZ2HnZJ0yQh0ll	192.168.202.136	33529	192.168.28.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_4.5	-	-	-	-	-
1332016065.680000	CTWHDfFzXZnBNHBq7	192.168.202.136	48999	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332015948.270000	CtRmqI1JbgTQECitIf	192.168.202.136	48992	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332011665.090000	CApkm63Pls4ZQYfWMk	192.168.202.68	43693	192.168.28.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.0	SSH-2.0-OpenSSH_4.5	-	-	-	-	-
1332014962.420000	C9eUXI3GSamu4rvinc	192.168.202.136	48897	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332014962.120000	CvGvWX2pW7tRDE45pl	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	-	-	-	-	-
1332014962.160000	CqRm1u2YhGenc5nUXi	192.168.202.136	48883	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332014961.950000	CkzM6a2xKKikrWRGv4	192.168.202.136	48869	192.168.21.253	22	undetermined	INBOUND	SSH-1.5-Nmap-SSH1-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332014961.840000	COsIst4WvDtA5CAD02	192.168.202.136	48861	192.168.21.253	22	undetermined	INBOUND	SSH-1.5-NmapNSE_1.0	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
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	-	-	-	-	-
1332014960.260000	CfSqT13pB1V35QL4Pl	192.168.202.136	56523	192.168.21.203	22	undetermined	INBOUND	SSH-1.5-Nmap-SSH1-Hostkey	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-
1332014960.250000	CaeoRv2zEj5ctI842i	192.168.202.136	60023	192.168.21.102	22	undetermined	INBOUND	SSH-1.5-Nmap-SSH1-Hostkey	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-
1332014883.950000	C8Bw6F2JD1ASZtOZlh	192.168.202.102	4380	192.168.21.253	22	undetermined	INBOUND	SSH-1.5-ssh.py	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332013747.050000	Cp7tq32KsWlYXpFKgd	192.168.202.141	8122	192.168.229.101	22	undetermined	INBOUND	-	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-
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	-	-	-	-	-
1332017154.520000	C0XOE9Wej5K5IETpj	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	-	-	-	-	-
1332016648.650000	C9QMWZ2HnZJ0yQh0ll	192.168.202.136	33529	192.168.28.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_4.5	-	-	-	-	-
1332016065.680000	CTWHDfFzXZnBNHBq7	192.168.202.136	48999	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-1.99-OpenSSH_4.5	-	-	-	-	-

Andando a filtrare soltanto gli nmap, negli ultimi 90 giorni non c’è alcun nmap che ha avuto successo, solo undetermined e failure.

Eventi

✓ 24 eventi (prima di 10/02/25 15:02:05,000)

20 per pagina ‹ Prec 1 2 Avanti ›

nmap Applica Esempio: 10.000 eventi Tutti gli eventi

_raw

1332014962.420000	C9eUXI3GSamu4rvinc	192.168.202.136	48897	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332014962.120000	CvGvWX2pW7tRDE45pl	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	-	-	-	-	-
1332014962.160000	CqRm1u2YhGenc5nUXi	192.168.202.136	48883	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332014961.950000	CkzM6a2xKKikrWRGv4	192.168.202.136	48869	192.168.21.253	22	undetermined	INBOUND	SSH-1.5-Nmap-SSH1-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332014961.840000	COsIst4WvDtA5CAD02	192.168.202.136	48861	192.168.21.253	22	undetermined	INBOUND	SSH-1.5-NmapNSE_1.0	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
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	-	-	-	-	-
1332014961.000000	C9Xd7rlrqMvvxdE7h	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	-	-	-	-	-
1332014961.040000	ChSj9guzUhPolkcA6	192.168.202.136	60076	192.168.21.102	22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-
1332014960.620000	C4wXMJ3QXd18LqQZZc	192.168.202.136	56543	192.168.21.203	22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-
1332014960.630000	CmS3YU3t21Hb2B7Bfc	192.168.202.136	60051	192.168.21.102	22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-
1332014960.260000	CfSqT13pB1V35QL4Pl	192.168.202.136	56523	192.168.21.203	22	undetermined	INBOUND	SSH-1.5-Nmap-SSH1-Hostkey	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-
1332014960.250000	CaeoRv2zEj5ctI842i	192.168.202.136	60023	192.168.21.102	22	undetermined	INBOUND	SSH-1.5-Nmap-SSH1-Hostkey	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-
1332014962.420000	C9eUXI3GSamu4rvinc	192.168.202.136	48897	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332014962.120000	CvGvWX2pW7tRDE45pl	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	-	-	-	-	-
1332014962.160000	CqRm1u2YhGenc5nUXi	192.168.202.136	48883	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332014961.950000	CkzM6a2xKKikrWRGv4	192.168.202.136	48869	192.168.21.253	22	undetermined	INBOUND	SSH-1.5-Nmap-SSH1-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332014961.840000	COsIst4WvDtA5CAD02	192.168.202.136	48861	192.168.21.253	22	undetermined	INBOUND	SSH-1.5-NmapNSE_1.0	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
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	-	-	-	-	-
1332014961.000000	C9Xd7rlrqMvvxdE7h	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	-	-	-	-	-
1332014961.040000	ChSj9guzUhPolkcA6	192.168.202.136	60076	192.168.21.102	22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-	-