
S10-L1

Analisi log con Splunk

Emanuele Benedetti | 10 febbraio 2025

Consegna

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.

Svolgimento

Come richiesto dalla consegna ho importato il file chiamato `ssh.log` in Splunk per eseguirne l'analisi.

Poiché il software non è riuscito ad estrarre tutti i campi del file, per eseguire un'analisi accurata, ho proceduto ad estrarre i campi in maniera manuale.

Nella pagina principale ho cliccato su *" + estrai nuovi campi "*, nella schermata che si apre ho selezionato un evento caratteristico da cui prendere i campi di interesse e cliccato su *"Avanti >"*. Ho quindi selezionato l'opzione *"Espressione regolare"* e ancora su *"Avanti >"*. Ho infine separato e aggiunto il nome ad ogni campo di interesse non riconosciuto in automatico da Splunk.

In questo modo siamo in grado di effettuare ricerche più precise e dettagliate per analizzare il file di log.

Nelle immagini che seguono ho riportato i passaggi appena descritti per facilitare la comprensione della creazione manuale dei campi.

(Negli screenshot non sono riportati la creazione dei campi relativi ad IP sorgente e destinazione e delle porte perché già eseguiti in precedenza).

Seleziona evento di esempio

Scegliere una source o un source type, selezionare un evento campione e fare clic su **Avanti** per continuare con il passaggio successivo. L'estrattore di campi userà l'evento per estrarre i campi. Ulteriori informazioni [\[?\]](#)

Prefetisco schivare lo stesso l'espressione regolare >

Source type
Dati ssh

Intervallo temporale
Ultima 90 giorni

1332817778.378000	CZH01136uZvNGuYl	192.168.282.136	56814	192.168.21.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-Jubuntu7	SSH-2.0-OpenSSH_5.3p1	Debian-lubuntu3	-	-	-	-

Eventi

✓ 1.000 evento (12/15/24 00:00:00.000 - 10/02/25 14:47:10.000)

20 per pagina < Prec 1 2 3 4 5 6 7 8 ... Avanti >

Filtro **Applica** Esempio: 1.000 eventi Tutti gli eventi

Raw

1332816697.210000	CyE9hc3vZQM9a1Bfbd	192.168.282.69	37812	192.168.28.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-Jubuntu7	SSH-2.0-OpenSSH_5.3p1	Debian-lubuntu3	-	-	-	-
1332817793.040000	CrUTzx1hVkiqFTTl	192.168.282.136	56815	192.168.21.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-Jubuntu7	SSH-2.0-OpenSSH_5.3p1	Debian-lubuntu3	-	-	-	-
1332817778.378000	CZH01136uZvNGuYl	192.168.282.136	56814	192.168.21.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-Jubuntu7	SSH-2.0-OpenSSH_5.3p1	Debian-lubuntu3	-	-	-	-
1332817154.520000	CR0E9WJ5K5IEtpj	192.168.282.136	56882	192.168.21.203	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-Jubuntu7	SSH-2.0-OpenSSH_5.3p1	Debian-lubuntu3	-	-	-	-
1332817111.470000	PMdntLdnc91nFnd8	192.168.282.136	47186	192.168.27.381	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-Jubuntu7	SSH-2.0-OpenSSH_5.3p1	Debian-lubuntu3	-	-	-	-

Attiva Windows
Passa a Impostazioni per attivare Windows.

Seleziona metodo

Indicare il metodo che si intende utilizzare per estrarre i campi. Ulteriori informazioni [\[?\]](#)

Prefetisco schivare lo stesso l'espressione regolare >

Source type
Dati ssh

1332817778.378000	CZH01136uZvNGuYl	192.168.282.136	56814	192.168.21.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-Jubuntu7	SSH-2.0-OpenSSH_5.3p1	Debian-lubuntu3	-	-	-	-

(.*)

Espressione regolare

Splunk Enterprise estrarrà i campi usando un'espressione regolare.

xlylz

Delimitatori

Splunk Enterprise estrarrà i campi utilizzando un delimitatore (come ad es. virgola, spazi o caratteri). Usare questo metodo per i dati delimitati, come i valori separati da virgola (file CSV).

Attiva Windows
Passa a Impostazioni per attivare Windows.

Seleziona campi

Evidenziare uno o più valori nell'evento di esempio per creare i campi. È possibile indicare un valore come obbligatorio, il che significa che deve esistere in un evento per fare in modo che l'espressione regolare vi corrisponda. Fare clic sui valori evidenziati nell'evento di esempio per modificarli. Per evidenziare il testo che fa già parte di un'estrazione esistente, disabilitare prima le estrazioni esistenti. Ulteriori informazioni [\[?\]](#)

1332817778.378000	CZH01136uZvNGuYl	192.168.282.136	56814	192.168.21.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-Jubuntu7	SSH-2.0-OpenSSH_5.3p1	Debian-lubuntu3	-	-	-	-

Mostra espressione regolare > **Visualizza in Ricerca** [\[?\]](#)

Anteprima

Se di seguito appaiono dei risultati non corretti, fare clic su un evento aggiuntivo per aggiungerlo al set degli eventi di esempio. Evidenziare i valori per migliorare l'estrazione. È possibile rimuovere i valori non corretti nel prossimo passaggio.

Eventi Timestamp ID_sessione Connessione SSH_versioneSorgente SSH_versioneDestinazione

✓ 1.000 evento (12/15/24 00:00:00.000 - 10/02/25 14:50:20.000)

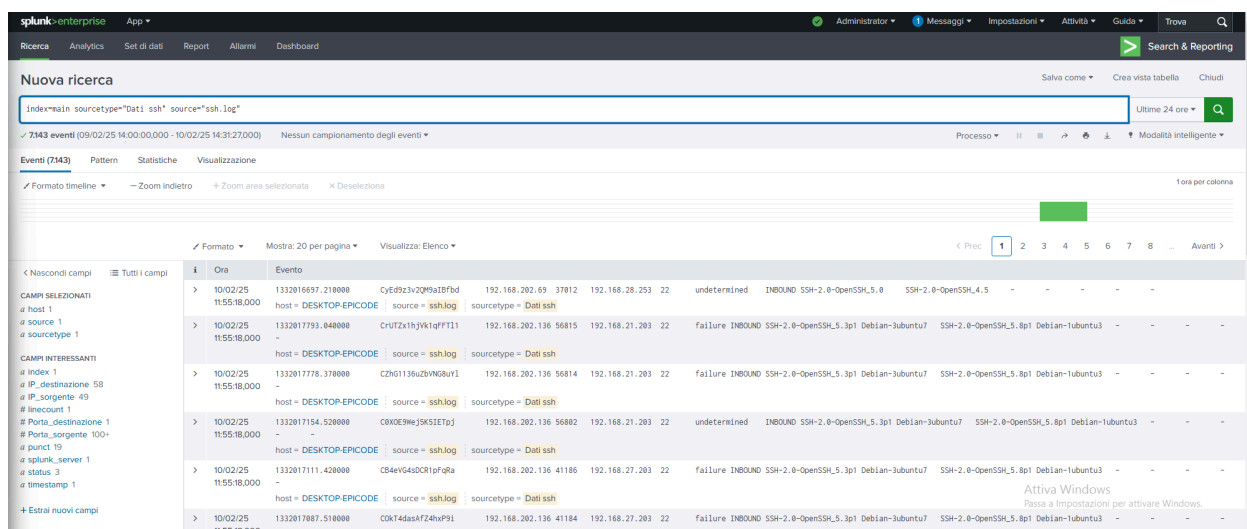
20 per pagina < Prec 1 2 3 4 5 6 7 8 ... Avanti >

Filtro **Applica** Esempio: 1.000 eventi Tutti gli eventi Corrispondenze Senza corrispondenze

Timestamp	ID_sessione	Connessione	SSH_versioneSorgente	SSH_versioneDestinazione
1332016697.210000	CyE9hc3vZQM9a1Bfbd	INBOUND	SSH-2.0-OpenSSH_5.3p1	SSH-2.0-OpenSSH_5.3p1
1332017793.040000	CrUTzx1hVkiqFTTl	INBOUND	SSH-2.0-OpenSSH_5.3p1	SSH-2.0-OpenSSH_5.3p1
1332017778.378000	CZH01136uZvNGuYl	INBOUND	SSH-2.0-OpenSSH_5.3p1	SSH-2.0-OpenSSH_5.3p1

Attiva Windows
Passa a Impostazioni per attivare Windows.

Ho iniziato l'analisi del file filtrando tramite la semplice query *index=main*
source="ssh.log" sourcetype="Dati ssh" che mi ha permesso di elencare tutte le entry.



Nuova ricerca
index=main sourcetype="Dati ssh" source="ssh.log"
7143 eventi (09/02/25 14:00:00.000 - 10/02/25 14:31:27.000) Nessun campionamento degli eventi

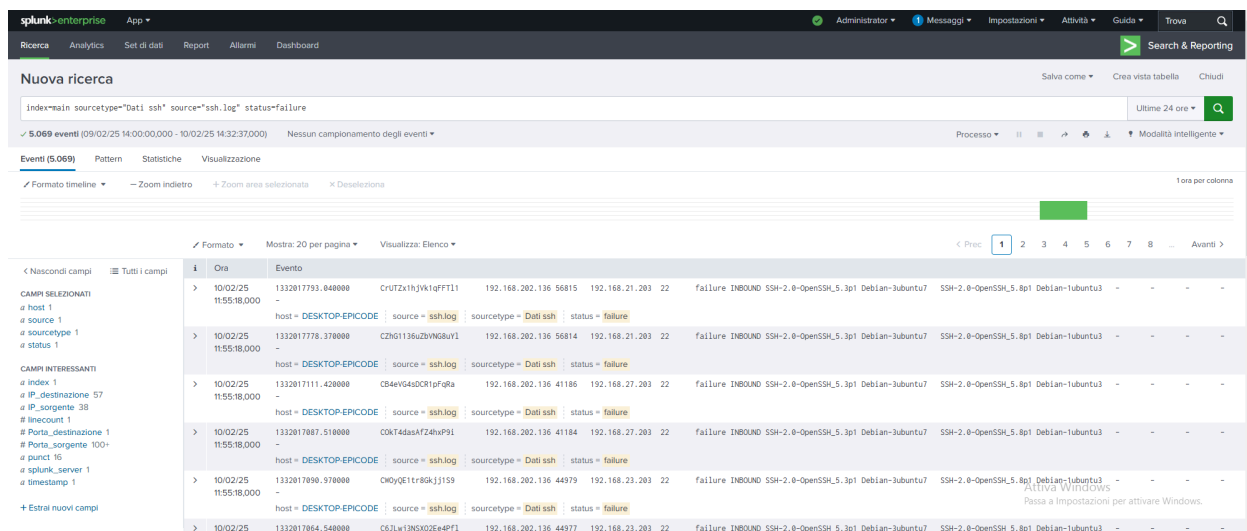
Formato timeline | Zoom indietro | Zoom area selezionata | Deselezione

Formato | Mostra: 20 per pagina | Visualizza: Elenco

	Ora	Evento
CAMPI SELEZIONATI	10/02/25 11:55:18,000	1332016697.210000 CyEd9z3vZQ9s1Bfbd host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
1 host 1	10/02/25 11:55:18,000	1332017793.840000 CrUTZx1hJYk1qFTT11 host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
1 source 1	10/02/25 11:55:18,000	1332017793.840000 CrUTZx1hJYk1qFTT11 host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
1 sourcetype 1	10/02/25 11:55:18,000	1332017793.840000 CrUTZx1hJYk1qFTT11 host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
CAMPI INTERESSANTI	10/02/25 11:55:18,000	1332017778.370000 CZbG1136uZbVNG8uY1 host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
1 index 1	10/02/25 11:55:18,000	1332017778.370000 CZbG1136uZbVNG8uY1 host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
1 IP_destinazione 58	10/02/25 11:55:18,000	1332017154.520000 C0X0E9weJ5K51ETpJ host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
1 IP_sorgente 49	10/02/25 11:55:18,000	1332017154.520000 C0X0E9weJ5K51ETpJ host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
1 Inaccount 1	10/02/25 11:55:18,000	1332017111.420000 CB4eVG4sDCR1pFqRa host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
1 Porta_destinazione 1	10/02/25 11:55:18,000	1332017111.420000 CB4eVG4sDCR1pFqRa host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
1 Porta_sorgente 100	10/02/25 11:55:18,000	1332017111.420000 CB4eVG4sDCR1pFqRa host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
1 punct 19	10/02/25 11:55:18,000	1332017111.420000 CB4eVG4sDCR1pFqRa host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
1 splunk_server 1	10/02/25 11:55:18,000	1332017111.420000 CB4eVG4sDCR1pFqRa host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
1 status 3	10/02/25 11:55:18,000	1332017111.420000 CB4eVG4sDCR1pFqRa host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
1 timestamp 1	10/02/25 11:55:18,000	1332017111.420000 CB4eVG4sDCR1pFqRa host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh
Altri nuovi campi	10/02/25 11:55:18,000	1332017887.510000 C0kT4dasAFZ4hxP9l host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh

Come possiamo vedere sono presenti moltissimi eventi (7143) e pertanto è necessario aggiungere ulteriori criteri di ricerca per riuscire a comprendere il file.

Utilizzando i campi creati in precedenza ho inizialmente filtrato per eventi *"failure"*, ovvero errori nell'autenticazione, tramite la query *index=main source="ssh.log" sourcetype="Dati ssh" status="failure"*.



Nuova ricerca
index=main sourcetype="Dati ssh" source="ssh.log" status=failure
5,069 eventi (09/02/25 14:00:00.000 - 10/02/25 14:32:37.000) Nessun campionamento degli eventi

Formato timeline | Zoom indietro | Zoom area selezionata | Deselezione

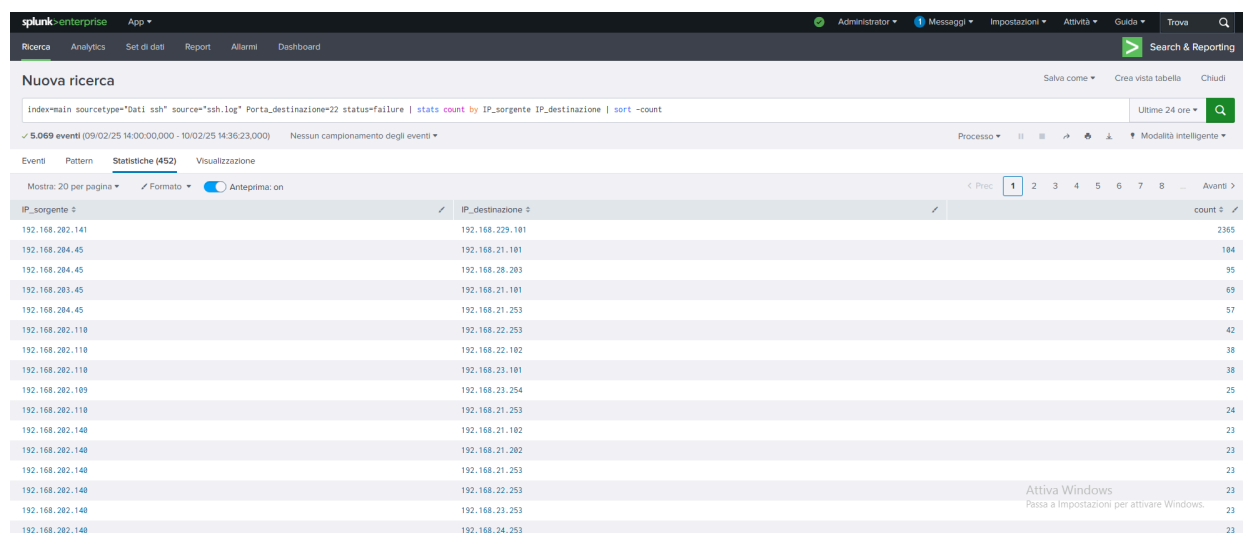
Formato | Mostra: 20 per pagina | Visualizza: Elenco

	Ora	Evento
CAMPI SELEZIONATI	10/02/25 11:55:18,000	1332017793.840000 CrUTZx1hJYk1qFTT11 host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
1 host 1	10/02/25 11:55:18,000	1332017793.840000 CrUTZx1hJYk1qFTT11 host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
1 source 1	10/02/25 11:55:18,000	1332017793.840000 CrUTZx1hJYk1qFTT11 host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
1 sourcetype 1	10/02/25 11:55:18,000	1332017793.840000 CrUTZx1hJYk1qFTT11 host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
1 status 1	10/02/25 11:55:18,000	1332017793.840000 CrUTZx1hJYk1qFTT11 host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
CAMPI INTERESSANTI	10/02/25 11:55:18,000	1332017111.420000 CB4eVG4sDCR1pFqRa host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
1 index 1	10/02/25 11:55:18,000	1332017111.420000 CB4eVG4sDCR1pFqRa host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
1 IP_destinazione 57	10/02/25 11:55:18,000	1332017111.420000 CB4eVG4sDCR1pFqRa host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
1 IP_sorgente 38	10/02/25 11:55:18,000	1332017111.420000 CB4eVG4sDCR1pFqRa host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
1 Inaccount 1	10/02/25 11:55:18,000	1332017887.510000 C0kT4dasAFZ4hxP9l host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
1 Porta_destinazione 1	10/02/25 11:55:18,000	1332017887.510000 C0kT4dasAFZ4hxP9l host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
1 Porta_sorgente 100	10/02/25 11:55:18,000	1332017887.510000 C0kT4dasAFZ4hxP9l host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
1 punct 16	10/02/25 11:55:18,000	1332017887.510000 C0kT4dasAFZ4hxP9l host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
1 splunk_server 1	10/02/25 11:55:18,000	1332017887.510000 C0kT4dasAFZ4hxP9l host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
1 timestamp 1	10/02/25 11:55:18,000	1332017887.510000 C0kT4dasAFZ4hxP9l host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure
Altri nuovi campi	10/02/25 11:55:18,000	1332017884.540000 C6JLwJ3NSX02Ee4PFI host = DESKTOP-EPICODE source = ssh.log sourcetype = Dati ssh status = failure

Il numero di eventi è sceso a 5069 ma per cercare di effettuare un'analisi ho concatenato più query tra di loro.

Per prima cosa ho deciso di creare una sorta di tabella che elencasse i tentativi di connessione fallita, separando e contando gli eventi in base ad IP sorgente ed IP destinazione.

Ho utilizzato la query di ricerca *index=main sourcetype="Dati ssh" source="ssh.log" status=failure | stats count by IP_sorgente IP_destinazione | sort -count* ordinando i risultati per numero di occorrenze.



The screenshot shows the Splunk Search & Reporting interface. The search bar contains the query: `index=main sourcetype="Dati ssh" source="ssh.log" status=failure | stats count by IP_sorgente IP_destinazione | sort -count`. The results are displayed in a table with 3 columns: `IP_sorgente`, `IP_destinazione`, and `count`. The table shows 20 rows of data, with the first row having a count of 2365. The interface also shows a search bar, a search button, and a search history section.

IP_sorgente	IP_destinazione	count
192.168.202.141	192.168.229.101	2365
192.168.204.45	192.168.21.101	184
192.168.204.45	192.168.28.203	95
192.168.203.45	192.168.21.101	69
192.168.204.45	192.168.21.253	57
192.168.202.110	192.168.22.253	42
192.168.202.110	192.168.22.102	38
192.168.202.110	192.168.23.101	38
192.168.202.109	192.168.23.254	25
192.168.202.110	192.168.21.253	24
192.168.202.140	192.168.21.102	23
192.168.202.140	192.168.21.202	23
192.168.202.140	192.168.21.253	23
192.168.202.140	192.168.22.253	23
192.168.202.140	192.168.23.253	23
192.168.202.140	192.168.24.253	23

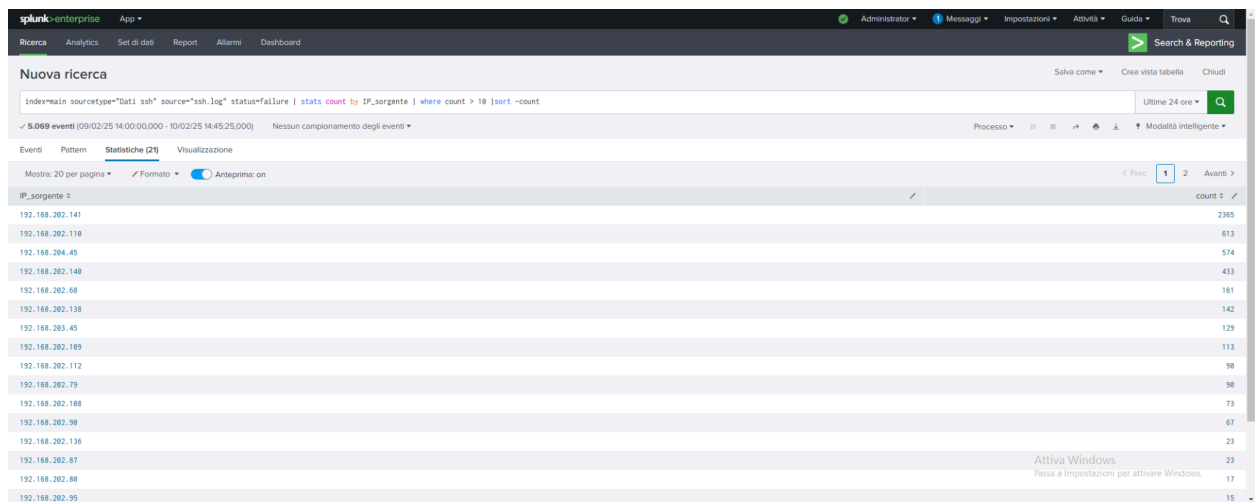
L'immagine mostra come questo comando ci permette di avere un'idea della distribuzione degli eventi, in particolare su 5069 eventi coerenti con la ricerca, 2365 sono tutti tentativi effettuati da un unico indirizzo IP (192.168.202.141) verso un unico target (192.168.229.101). Da questo risultato possiamo evincere ad esempio che l'host ha tentato un attacco brute force (o di tipo dizionario) verso il server ssh.

Anche le entrate successive mostrano un elevato numero di tentativi di accesso falliti e potrebbero essere nuovamente indice di tentato attacco brute force.

Ho quindi utilizzato un nuovo comando di ricerca per filtrare gli indirizzi IP sorgente in base al numero di tentativi di login falliti, utilizzando 10 come valore limite per cui

mostrare i risultati. L'obiettivo è riuscire a capire quali sono gli indirizzi che con buona probabilità hanno tentato un attacco di forza bruta verso il server ssh.

La query di ricerca che ho utilizzato è *index=main sourcetype="Dati ssh" source="ssh.log" status=failure | stats count by IP_sorgente | where count > 10 | sort -count*.



The screenshot shows the Splunk Enterprise Search & Reporting interface. The search bar contains the query: `index=main sourcetype="Dati ssh" source="ssh.log" status=failure | stats count by IP_sorgente | where count > 10 | sort -count`. The results are displayed in a table with 21 rows, each representing an IP address and its corresponding count of failed attempts. The table is titled "Nuova ricerca" and shows 5,069 events. The search results are sorted by count in descending order.

IP_sorgente	count
192.168.202.141	2365
192.168.202.118	613
192.168.204.45	574
192.168.202.140	433
192.168.202.68	161
192.168.202.138	142
192.168.203.45	129
192.168.202.109	113
192.168.202.112	98
192.168.202.79	98
192.168.202.108	73
192.168.202.98	67
192.168.202.136	23
192.168.202.87	23
192.168.202.88	17
192.168.202.95	15

L'immagine mostra che in base al criterio (> 10 tentativi falliti verso lo stesso endpoint) ci sono 21 indirizzi IP sospetti.