



Splunk

DNS LOG ANALYSIS

Descrizione del progetto

Prenderemo in esame un log dns «raw», vedremo come estrarre dei campi grazie alle funzioni built-in di Splunk, per poi farne una analisi vedendo alcune informazioni che possiamo ricavare.

Caricamento del file di log

Clicchiamo su «aggiungi dati» scegliamo il path dove risiede il file, diamo il nome al source type, confermiamo gli altri campi e carichiamo il file per poter effettuare le ricerche su di esso tramite il modulo Search and Reporting.

The screenshot displays the Splunk Enterprise web interface. On the left, the 'Ricerca' (Search) section is visible. In the center, the 'Aggiungi dati' (Add Data) menu is open, showing a list of categories and their associated data sources. On the right, the 'Salva source type' (Save source type) dialog is shown, with the following fields filled:

- Nome** (Name): DNS log
- Descrizione** (Description): first dns log data
- Categoria** (Category): Personalizzata (Custom)
- App** (App): Search & Reporting

At the bottom right of the dialog are two buttons: 'Annulla' (Cancel) and 'Salva' (Save).

Aggiungi dati menu items:

- KNOWLEDGE**
 - Ricerche, report e allarmi
 - Modelli dati
 - Event type
 - Tag
 - Campi
 - Lookup
 - Interfaccia utente
 - Azioni di allarme
 - Ricerca avanzata
 - Tutte le configurazioni
- SISTEMA**
 - Impostazioni server
 - Comandi del server
 - Gestione report sullo stato di salute
 - Strumentazione
 - Licenze
 - Gestione dei carichi di lavoro
 - Mobile settings
- DATI**
 - Input dati
 - Inoltro e ricezione
 - Indici
 - Sommari di accelerazione
 - report
 - Source type
 - Azioni di inserimento
- AMBIENTE DISTRIBUITO**
 - Clustering di indexer
 - Gestione forwarder
 - Ricerca federata
 - Ricerca distribuita
- UTENTI E AUTENTICAZIONE**
 - Ruoli
 - Utenti
 - Token
 - Gestione password
 - Metodi di autenticazione

Analisi

I campi estratti in automatico risultano essere riduttivi ai fini dell'analisi, per cui possiamo procedere con l'estrazione dei campi associati agli eventi quali: dominio interessato, source e destination ip ecc.

Possiamo fare ciò cliccando su «Estrai nuovi Campi»

< Nascondi campi

☰ Tutti i campi

CAMPI SELEZIONATI

a host 1

a source 1

a sourcetype 1

CAMPI INTERESSANTI

a index 1

linecount 10

a punct 100+

a splunk_server 1

a timestamp 1

11 campi in più

+ Estrai nuovi campi

Estrazione dei campi: selezione di un evento campione.

The screenshot shows the Splunk Field Extractor interface. At the top, a progress bar indicates the current step is 'Seleziona campi', with the 'Avanti >' button circled in red. Below the progress bar, the 'Seleziona evento di esempio' section is active, showing a 'DNS log' source type and a 'Ultima 90 giorni' time range. A sample event is displayed in a blue bar. The 'Eventi' section below shows a list of events with a filter and a table of event details. The table has columns for event ID, source, destination, protocol, port, and various fields. The first row of the table is highlighted.

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](#)

Preferisco scrivere lo stesso l'espressione regolare >

Source type
DNS log

Intervallo temporale
Ultima 90 giorni

1332017991.970000 Cw500TGmBFF5z1Rc9 192.168.202.122 137 192.168.202.255 137 udp 33707 LABADMIN-641491 1 C_INTERNET 32 NB - - F F T F 1 - - F

Eventi

✓ 1.000 evento (04/06/24 00:00:00,000 - 02/09/24 19:17:12,000) 20 per pagina < Prec 1 2 3 4 5 6 7 8 ... Avanti >

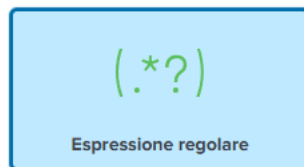
filto Esempio: 1.000 eventi Tutti gli eventi

_raw	...																			
1332017991.970000	Cw500TGmBFF5z1Rc9	192.168.202.122 137	192.168.202.255 137	udp	33707	LABADMIN-641491 1	C_INTERNET	32	NB	-	-	F	F	T	F	1	-	-	F	
1332017979.080000	CQnrcF1yLbtvjQbS8	192.168.202.83	45561	192.168.207.4	53	udp	12572	44.206.168.192.in-addr.arpa	1	C_INTERNET	12	PTR	3	NXDOMAIN	F	F	T	F	0	-
1332017959.830000	C4zDh93z81GYT1dq2k	192.168.202.88	60538	192.168.206.44	53	udp	36843	dr._dns-sd._udp.0.48.16.172.in-addr.arpa	1	C_INTERNET	12	PTR	5	REFUSED F	F	T	F	0	-	
1332017959.830000	CGBRgg3GyzwSH1wkB7	192.168.202.88	58547	192.168.206.44	53	udp	30842	dr._dns-sd._udp.0.202.168.192.in-addr.arpa	1	C_INTERNET	12	PTR	5	REFUSED F	F	T	F	0	-	
1332017959.830000	C1ZL144oVCIMvJgqb	192.168.202.88	58045	192.168.206.44	53	udp	28561	b._dns-sd._udp.0.48.16.172.in-addr.arpa	1	C_INTERNET	12	PTR	5	REFUSED F	F	T	F	0	-	
1332017959.830000	C0n0E3NUMg9TxJRsd	192.168.202.88	65208	192.168.206.44	53	udp	50791	1b._dns-sd._udp.0.48.16.172.in-addr.arpa	1	C_INTERNET	12	PTR	5	REFUSED F	F	T	F	0	-	

Estrazione dei campi

In base e grazie all'evento campione effettuiamo un «parsing» sul file di log, logicamente conoscendo la struttura di questi logs e i pattern che seguono.

Qui sotto riportiamo un esempio individuando il source ip, lo faremo anche per altri campi sullo stesso log e nella stessa sessione; sarebbe buona pratica estrarre però un campo per volta.



Splunk Enterprise estrarrà i campi usando un'espressione regolare.

x|y|z

Delimitatori

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

Seleziona campi

Evidenziare uno o più valori nell'evento di esempio per creare i campi. È possibile indicare il testo che fa già parte di un'estrazione esistente, disabilitare prima le e

1332017991.970000 CwS00TGmBFF5z1Rc9 192.168.202.122 137

Anteprima

Se di seguito appaiono dei risultati non co

Eventi

✓ 1.000 evento (04/06/24 00:00:00,000 - C

Estrai

Richiedi

Nome campo

src_ip

Valore di esempio

192.168.202.122

Add Extraction

Estrazione dei 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](#)

[Mostra espressione regolare >](#)

[Visualizza in Ricerca](#)

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

Eventi ● src_ip ● src_port ● dst_ip ● dst_port ● Domain

	_raw											src_ip	src_port	dst_ip	dst_port	Domain
✓	1332017991.970000 LABADMIN-641491 F	CwS00TgmBFF5zIRc9 1 C_INTERNET	192.168.202.122 32 NB -	137 - F F T F	192.168.202.255	137	udp 1 - -	33707	-	192.168.202.122	137	192.168.202.255	137	LABADMIN-641491		
✓	1332017979.080000 44.206.168.192.in-addr.arpa - - F	CQnrcF1yLbtvjQbS8 1 C_INTERNET	192.168.202.83 12 PTR	45561 3 NXDOMAIN	192.168.207.4	53	udp F	12572 0		192.168.202.83	45561	192.168.207.4	53	44.206.168.192.in-addr.arpa		
✓	1332017959.830000 dr_dns-sd._udp.0.48.16.172.in-addr.arpa 0 - - T	C4zDh93z81GYTldq2k 1 C_INTERNET	192.168.202.88 12 PTR	60538 5 REFUSED F	192.168.206.44	53	udp F T F	36843		192.168.202.88	60538	192.168.206.44	53	dr_dns-sd._udp.0.48.16.172.in-addr.arpa		

Estrazione dei campi: nuovi campi interessanti

In automatico in base ai campi selezionati viene elaborata la regular expression corrispondente, fatto ciò potremo visualizzare i nuovi campi generati come in basso a destra.

Salva

Assegnare un nome all'estrazione e impostare le autorizzazioni.

Nome estrazioni **EXTRACT-**

Proprietario **splunktest**

App **search**

Autorizzazioni ☒ Proprietario ☐ App ☐ Tutte le app

Source type **DNS log**

Evento di esempio 1332017979.080000 CQnrcF1yLbtvjQbS8 192.168.202.83 45561 192.168.207.4 53 udp
12572 44.206.168.192.in-addr.arpa 1 C_INTERNET 12 PTR 3 NXDOMAIN F
F T F 0 - - F

Campi **src_ip,src_port,dst_ip,dst_port,Domain**

Espressione regolare **^(?:[^\t\n]*\t){2}(?P<src_ip>[^\t+])\t(?P<src_port>\d+)\t(?P<dst_ip>[^\t+])\t(?P<dst_port>[^\t+])\t[w+|t|d+]\t(?P<Domain>[^\t]+)**

CAMPI SELEZIONATI

a host 1
a source 1
a sourcetype 1

CAMPI INTERESSANTI

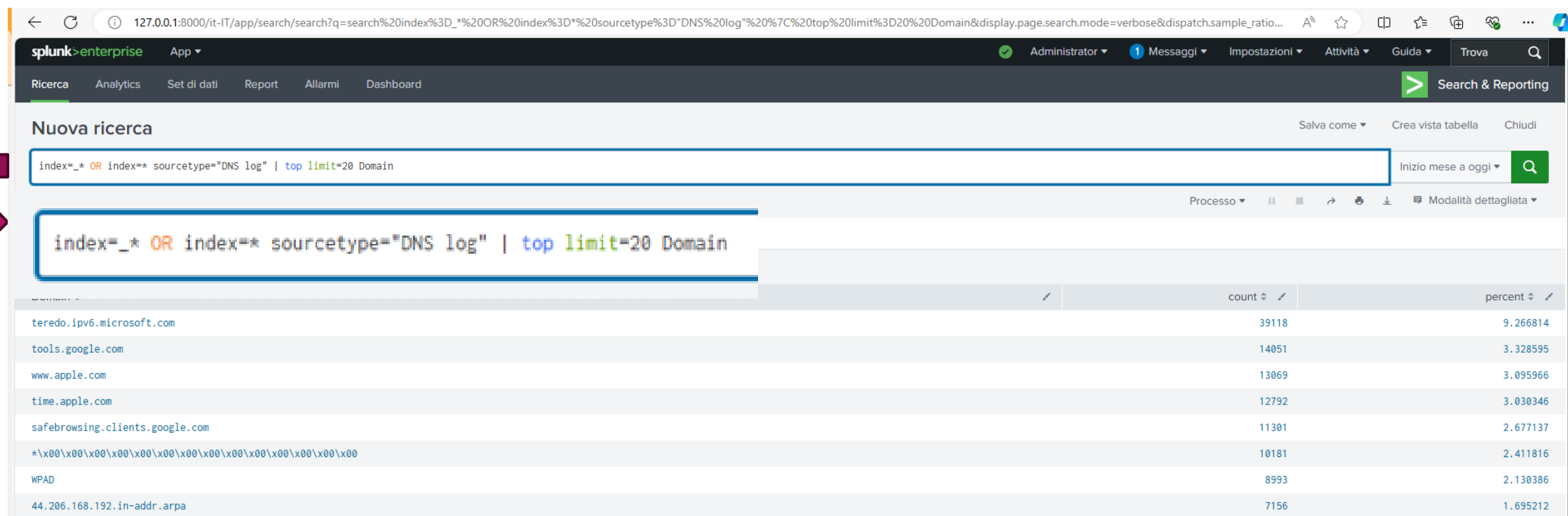
a Domain 100+
a dst_ip 100+
dst_port 4
a index 1
linecount 10
a punct 100+
a splunk_server 1
a src_ip 100+
src_port 100+
a timestamp 1

11 campi in più

+ Estrai nuovi campi

Analisi del log

Ora che abbiamo più campi su cui lavorare possiamo procedere con l'analisi vera e propria, per esempio vedere i primi 20 domini più cercati, o in ogni caso isolare l'analisi dei domini può essere utile in caso di ransomware per vedere a quale server C2 si è collegata la macchina infetta.

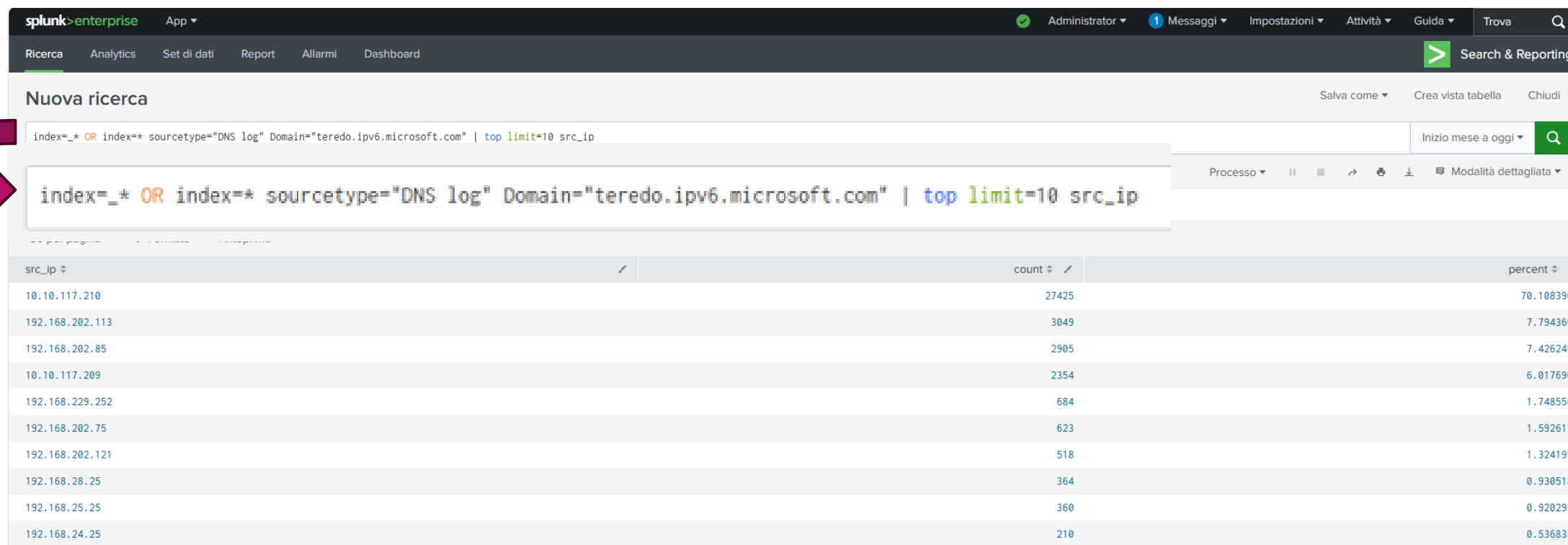


The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index=*_* OR index=* sourcetype="DNS log" | top limit=20 Domain`. A red arrow points to the search bar. Below the search bar, the same query is displayed in a code editor. The results are shown in a table with columns for domain, count, and percent.

	count	percent
teredo.ipv6.microsoft.com	39118	9.266814
tools.google.com	14051	3.328595
www.apple.com	13069	3.095966
time.apple.com	12792	3.030346
safebrowsing.clients.google.com	11301	2.677137
*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00	10181	2.411816
WPAD	8993	2.130386
44.206.168.192.in-addr.arpa	7156	1.695212

Analisi del log

Un altro caso potrebbe essere quello che individuiamo un dominio sospetto e vogliamo vedere quali macchine hanno effettuato più richieste verso di esso.

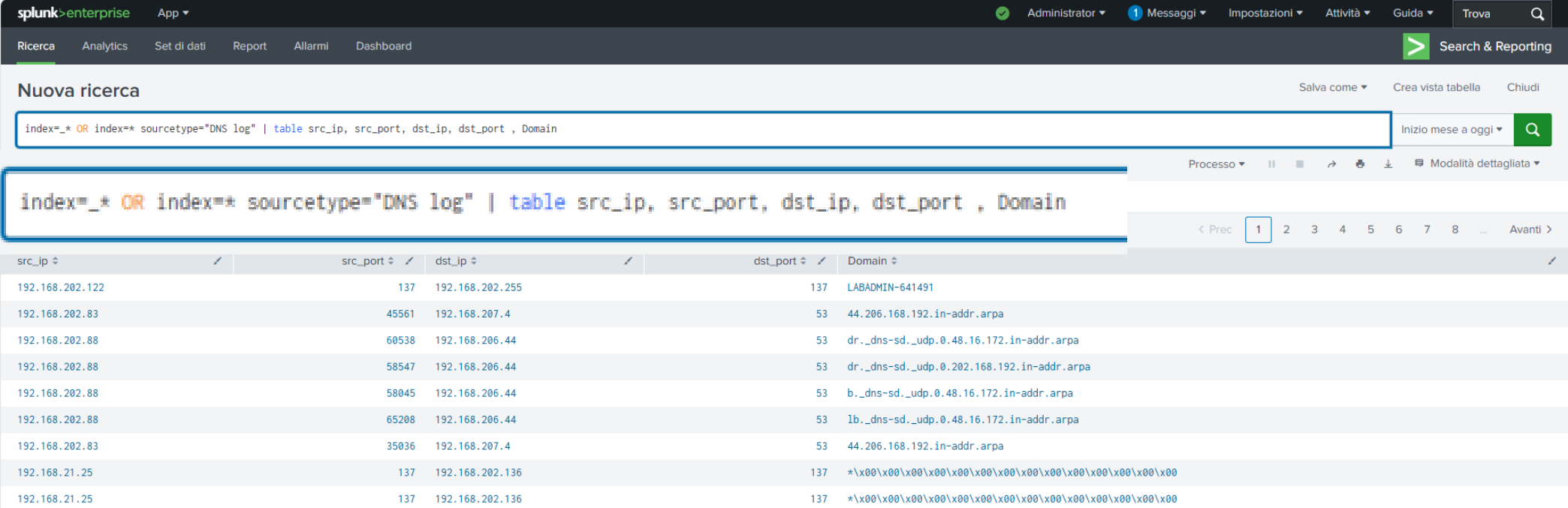


The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index=_* OR index=* sourcetype="DNS log" Domain="teredo.ipv6.microsoft.com" | top limit=10 src_ip`. A red arrow points to the search bar. The results table shows the top 10 source IP addresses and their corresponding counts and percentages.

src_ip	count	percent
10.10.117.210	27425	70.108390
192.168.202.113	3049	7.794366
192.168.202.85	2905	7.426249
10.10.117.209	2354	6.017690
192.168.229.252	684	1.748556
192.168.202.75	623	1.592617
192.168.202.121	518	1.324199
192.168.28.25	364	0.930518
192.168.25.25	360	0.920292
192.168.24.25	210	0.536837

Analisi del log

Possiamo infine per esempio creare una tabella dove visualizziamo ip e porte di sorgente e di destinazione ed individuare i server dns (banalmente se più source ip fanno richiesta ad un altro ip sulla porta 53 sarà un dns server).



The screenshot shows the Splunk Enterprise interface. The search bar contains the query: `index=*_ OR index=* sourcetype="DNS log" | table src_ip, src_port, dst_ip, dst_port , Domain`. Below the search bar, a table displays the results of the search. The table has columns for `src_ip`, `src_port`, `dst_ip`, `dst_port`, and `Domain`. The results show various source IP addresses and ports, with many requests directed to destination IP 192.168.206.44 on port 53, which is identified as a DNS server.

src_ip	src_port	dst_ip	dst_port	Domain
192.168.202.122	137	192.168.202.255	137	LABADMIN-641491
192.168.202.83	45561	192.168.207.4	53	44.206.168.192.in-addr.arpa
192.168.202.88	60538	192.168.206.44	53	dr._dns-sd._udp.0.48.16.172.in-addr.arpa
192.168.202.88	58547	192.168.206.44	53	dr._dns-sd._udp.0.202.168.192.in-addr.arpa
192.168.202.88	58045	192.168.206.44	53	b._dns-sd._udp.0.48.16.172.in-addr.arpa
192.168.202.88	65208	192.168.206.44	53	1b._dns-sd._udp.0.48.16.172.in-addr.arpa
192.168.202.83	35036	192.168.207.4	53	44.206.168.192.in-addr.arpa
192.168.21.25	137	192.168.202.136	137	*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
192.168.21.25	137	192.168.202.136	137	*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00