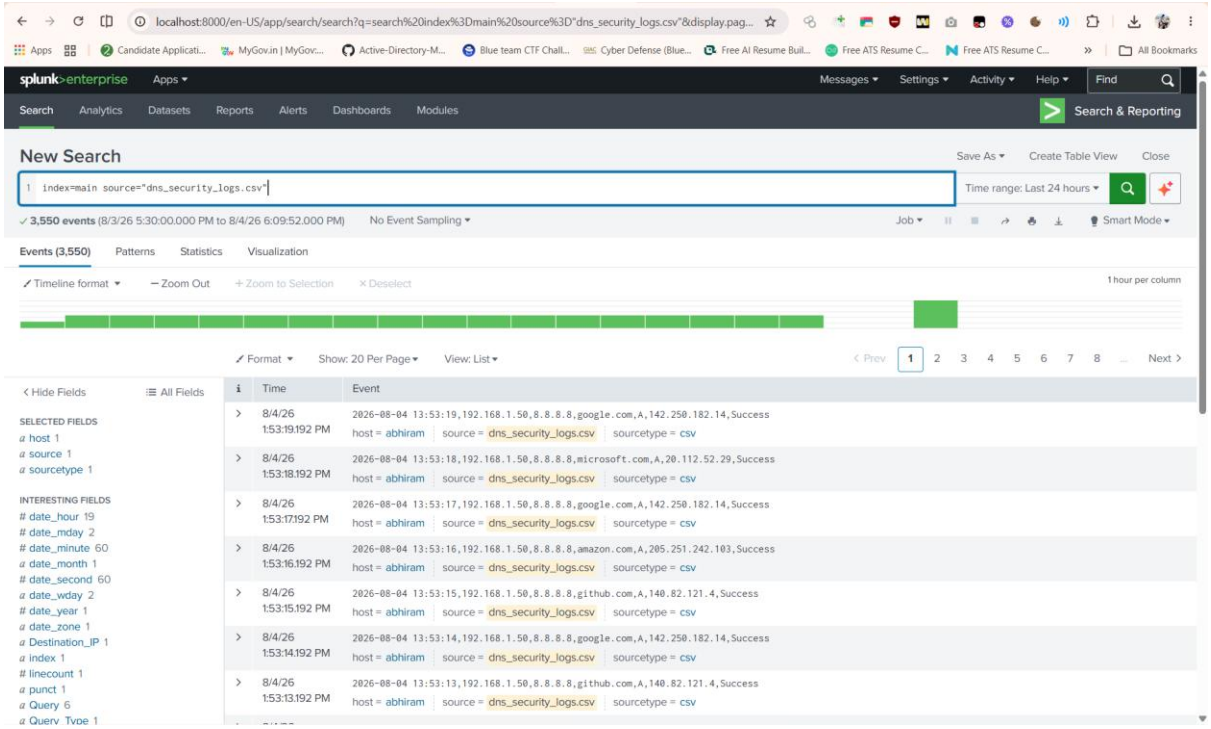
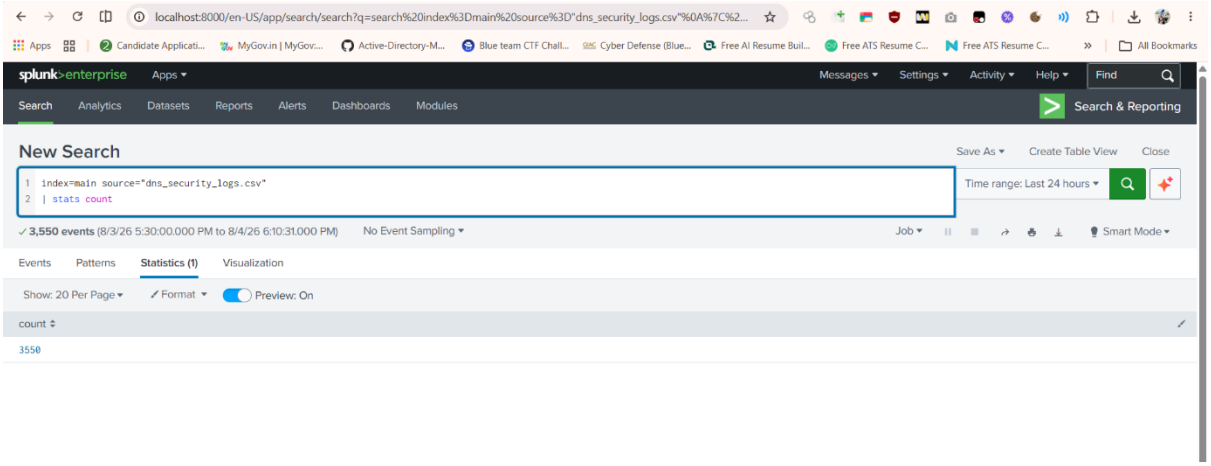
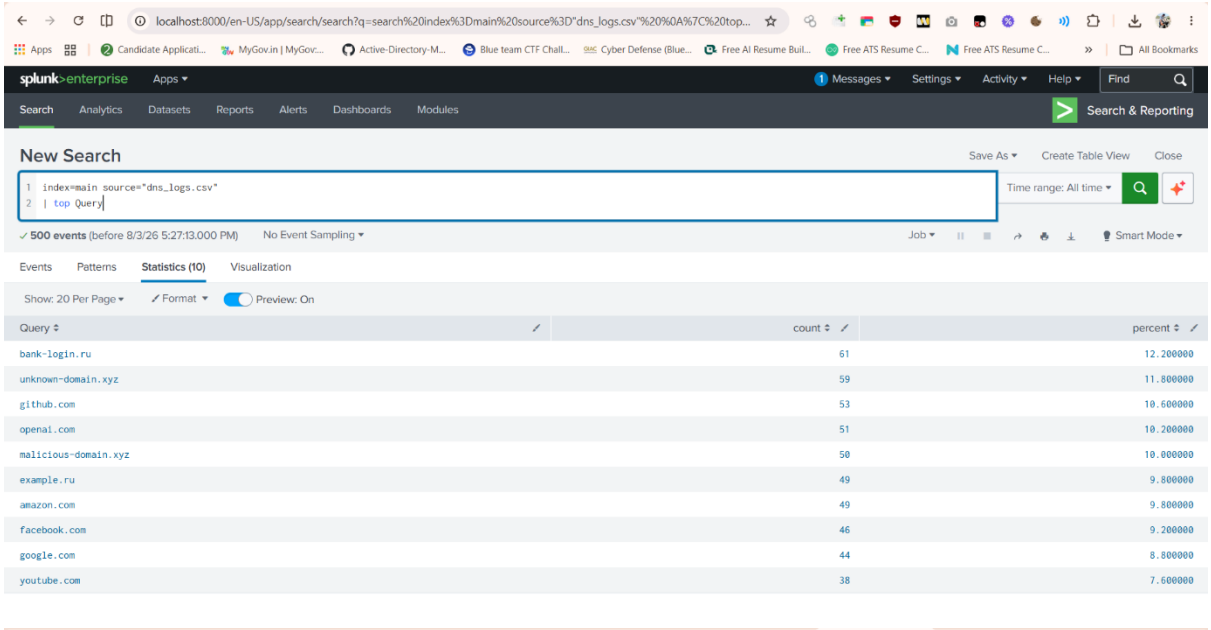
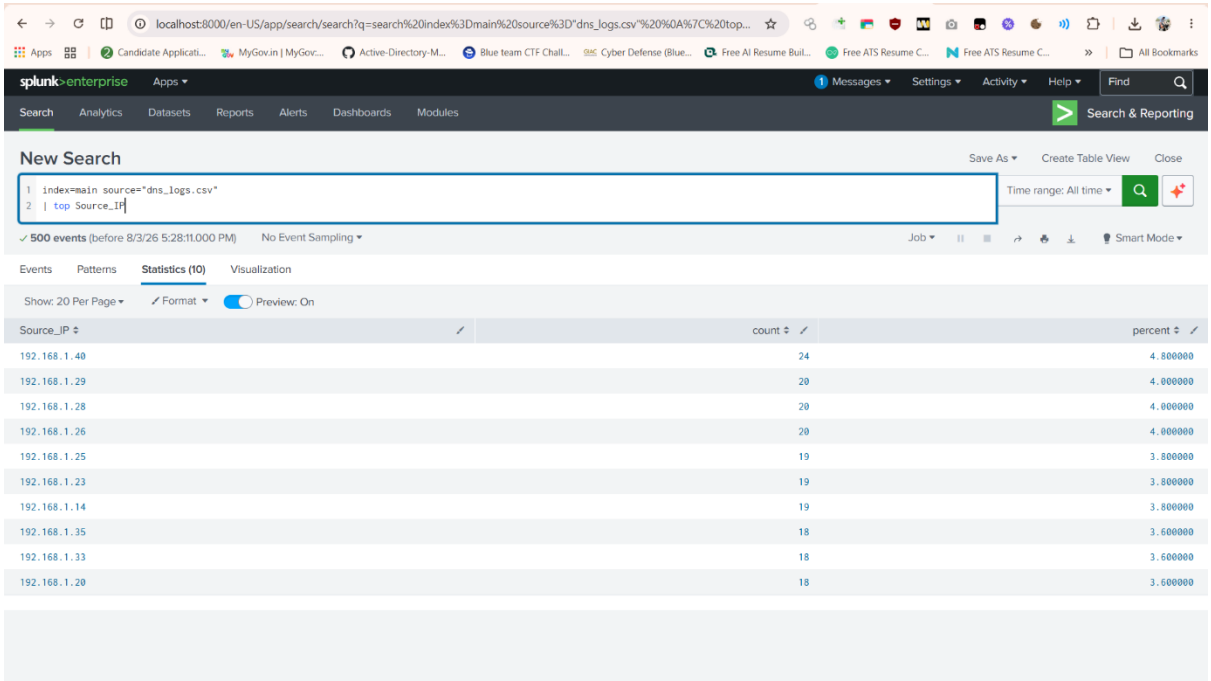

localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20source%3D"dns_security_logs.csv"&display.pag...
splunk>enterprise
Apps
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Modules
Search & Reporting
New Search
Save As
Create Table View
Close
index=main source="dns_security_logs.csv"
Time range: Last 24 hours
3,550 events (8/3/26 5:30:00.000 PM to 8/4/26 6:09:52.000 PM)
No Event Sampling
Job
Smart Mode
Events (3,550)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 20 Per Page
View: List
Prev
1 2 3 4 5 6 7 8 ...
Next
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
date_hour 19
date_mday 2
date_minute 60
date_month 1
date_second 60
date_wday 2
date_year 1
date_zone 1
Destination_IP 1
index 1
linecount 1
punct 1
Query 6
Query_Type 1
Time
Event
8/4/26 1:53:19.192 PM
2026-08-04 13:53:19,192.168.1.50,8.8.8.8,google.com,A,142.250.182.14,Success
host = abhiram source = dns_security_logs.csv sourcetype = csv
8/4/26 1:53:18.192 PM
2026-08-04 13:53:18,192.168.1.50,8.8.8.8,microsoft.com,A,20.112.52.29,Success
host = abhiram source = dns_security_logs.csv sourcetype = csv
8/4/26 1:53:17.192 PM
2026-08-04 13:53:17,192.168.1.50,8.8.8.8,google.com,A,142.250.182.14,Success
host = abhiram source = dns_security_logs.csv sourcetype = csv
8/4/26 1:53:16.192 PM
2026-08-04 13:53:16,192.168.1.50,8.8.8.8,amazon.com,A,205.251.242.103,Success
host = abhiram source = dns_security_logs.csv sourcetype = csv
8/4/26 1:53:15.192 PM
2026-08-04 13:53:15,192.168.1.50,8.8.8.8,github.com,A,140.82.121.4,Success
host = abhiram source = dns_security_logs.csv sourcetype = csv
8/4/26 1:53:14.192 PM
2026-08-04 13:53:14,192.168.1.50,8.8.8.8,google.com,A,142.250.182.14,Success
host = abhiram source = dns_security_logs.csv sourcetype = csv
8/4/26 1:53:13.192 PM
2026-08-04 13:53:13,192.168.1.50,8.8.8.8,github.com,A,140.82.121.4,Success
host = abhiram source = dns_security_logs.csv sourcetype = csv

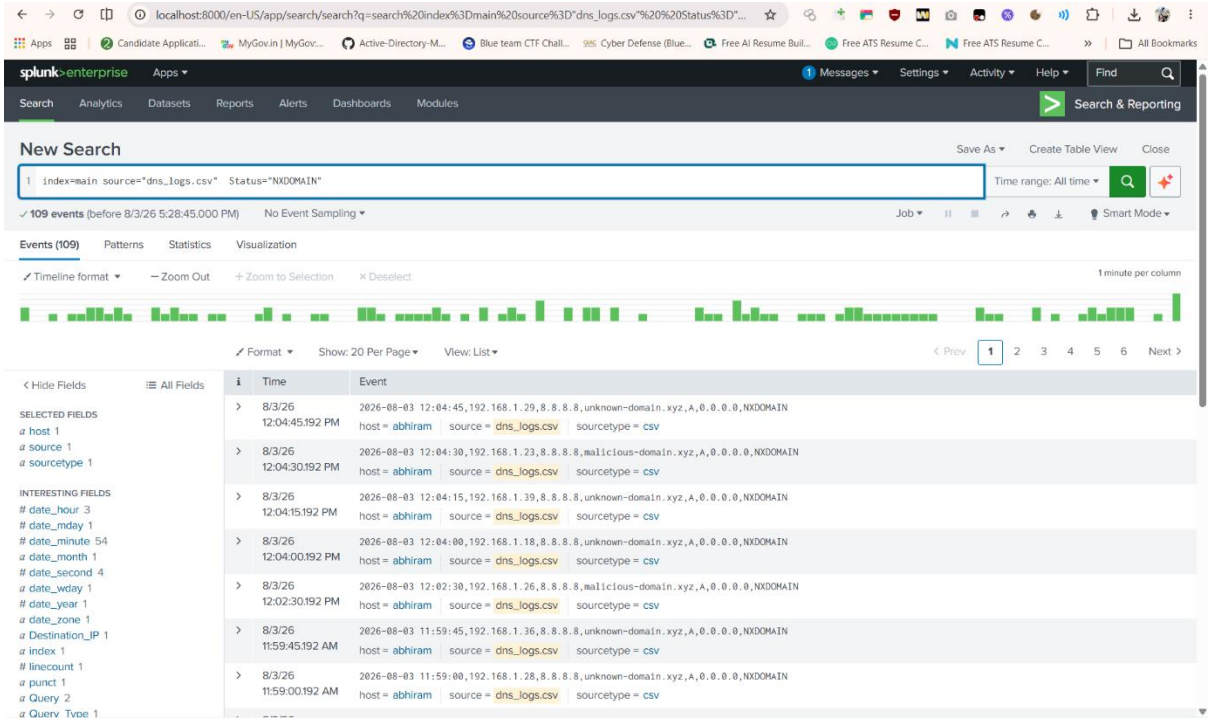

localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20source%3D"dns_security_logs.csv"%0A%7C%2...
splunk>enterprise
Apps
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Modules
Search & Reporting
New Search
Save As
Create Table View
Close
index=main source="dns_security_logs.csv"
| stats count
Time range: Last 24 hours
3,550 events (8/3/26 5:30:00.000 PM to 8/4/26 6:10:31.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (1)
Visualization
Show: 20 Per Page
Format
Preview: On
count
3550

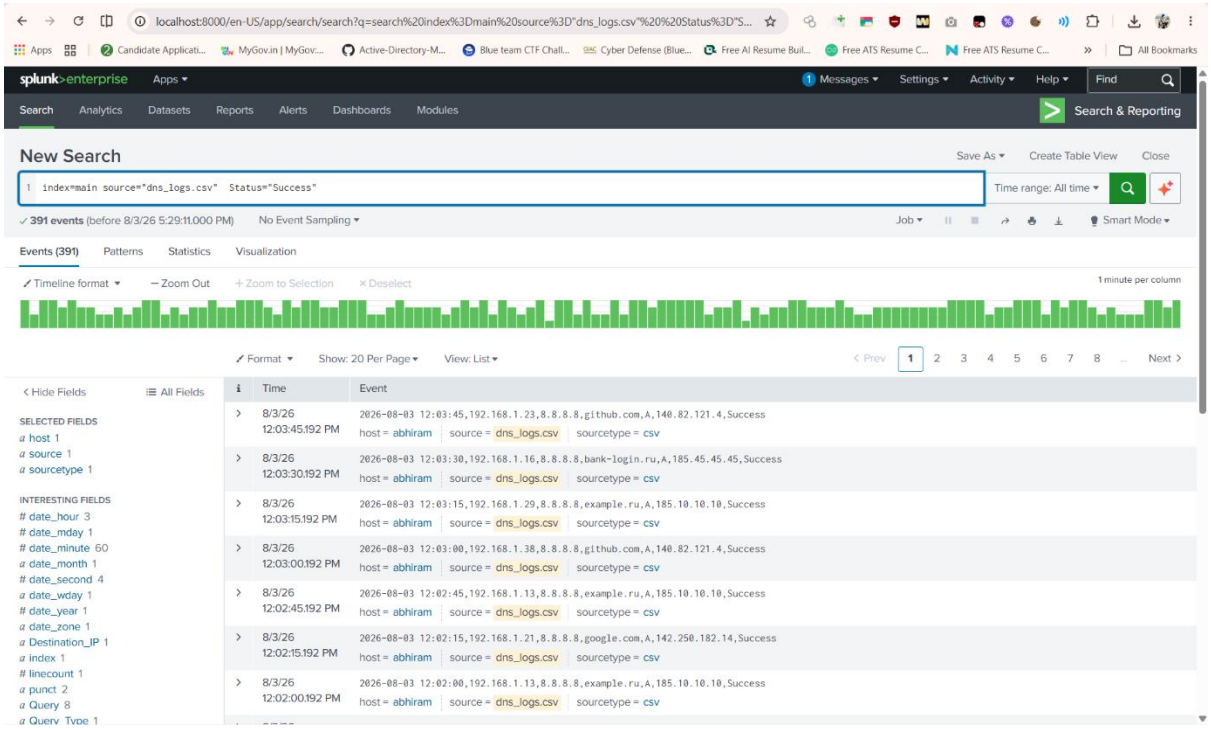


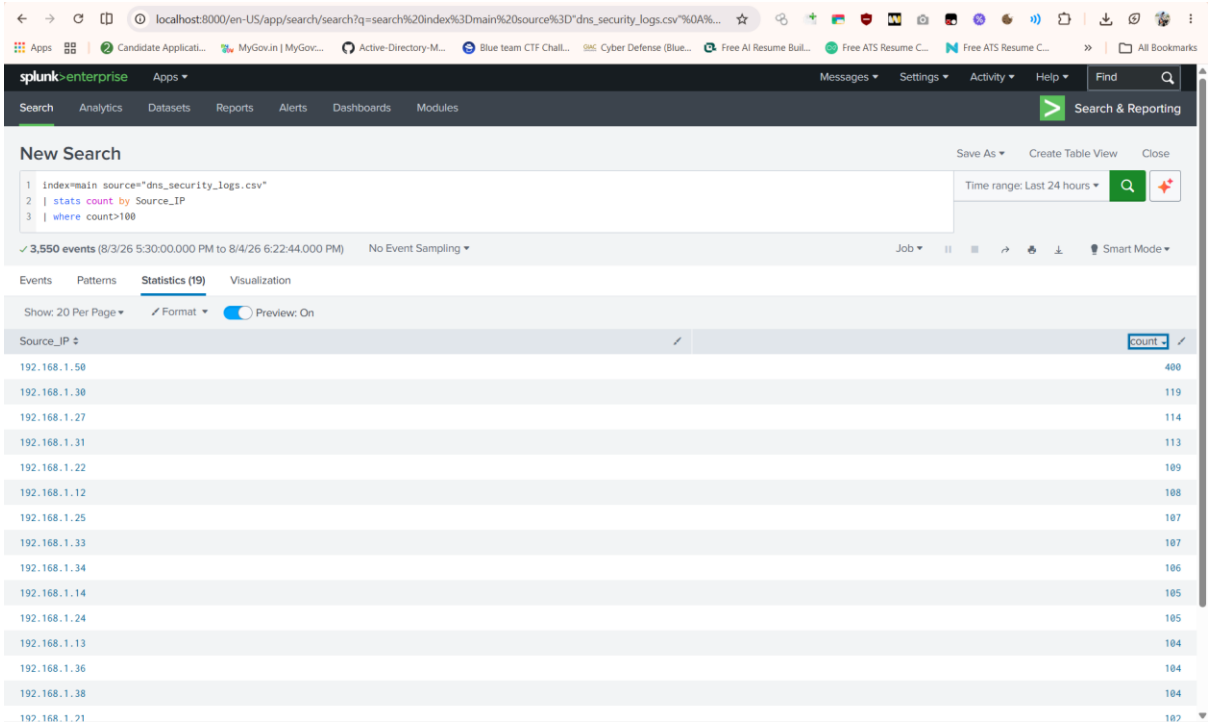
Query	count	percent
bank-login.ru	61	12.200000
unknown-domain.xyz	59	11.800000
github.com	53	10.600000
openai.com	51	10.200000
malicious-domain.xyz	50	10.000000
example.ru	49	9.800000
amazon.com	49	9.800000
facebook.com	46	9.200000
google.com	44	8.800000
youtube.com	38	7.600000

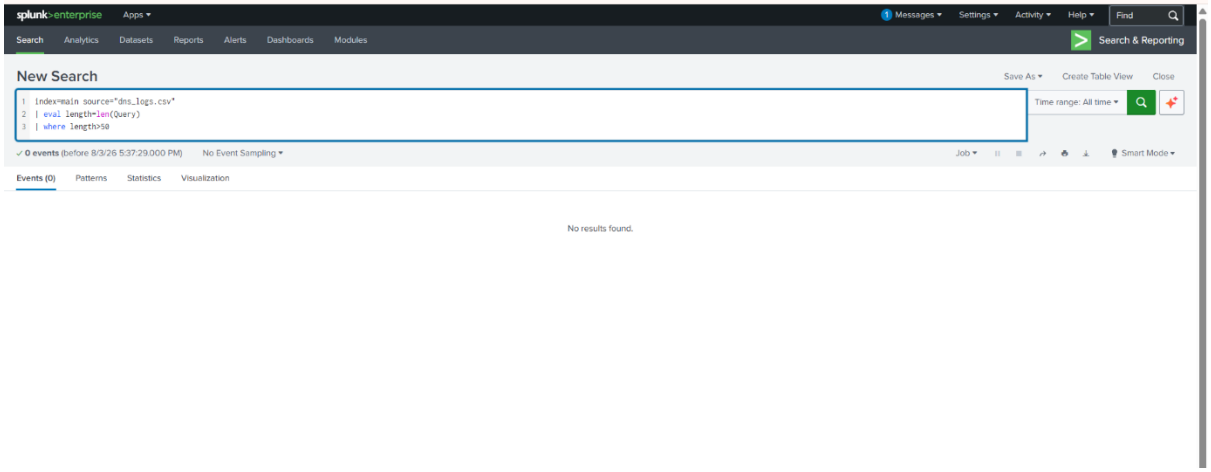


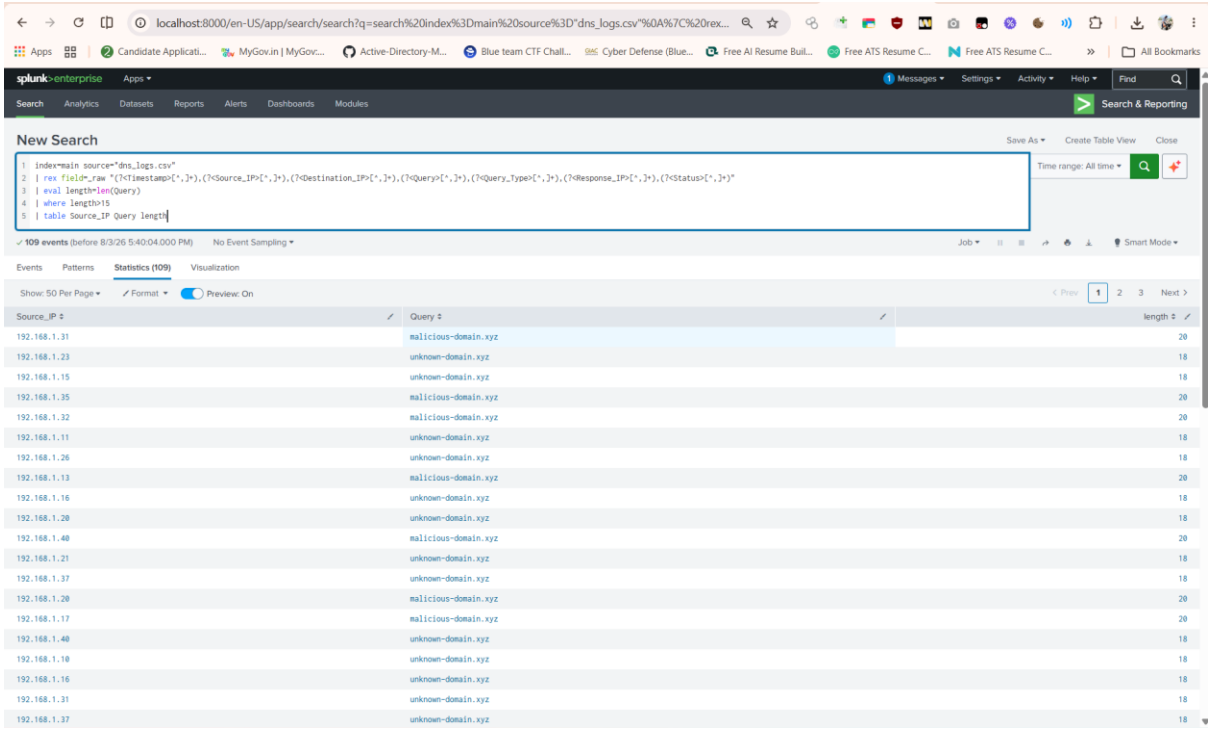
Source_IP	count	percent
192.168.1.40	24	4.800000
192.168.1.29	20	4.000000
192.168.1.28	20	4.000000
192.168.1.26	20	4.000000
192.168.1.25	19	3.800000
192.168.1.23	19	3.800000
192.168.1.14	19	3.800000
192.168.1.35	18	3.600000
192.168.1.33	18	3.600000
192.168.1.20	18	3.600000

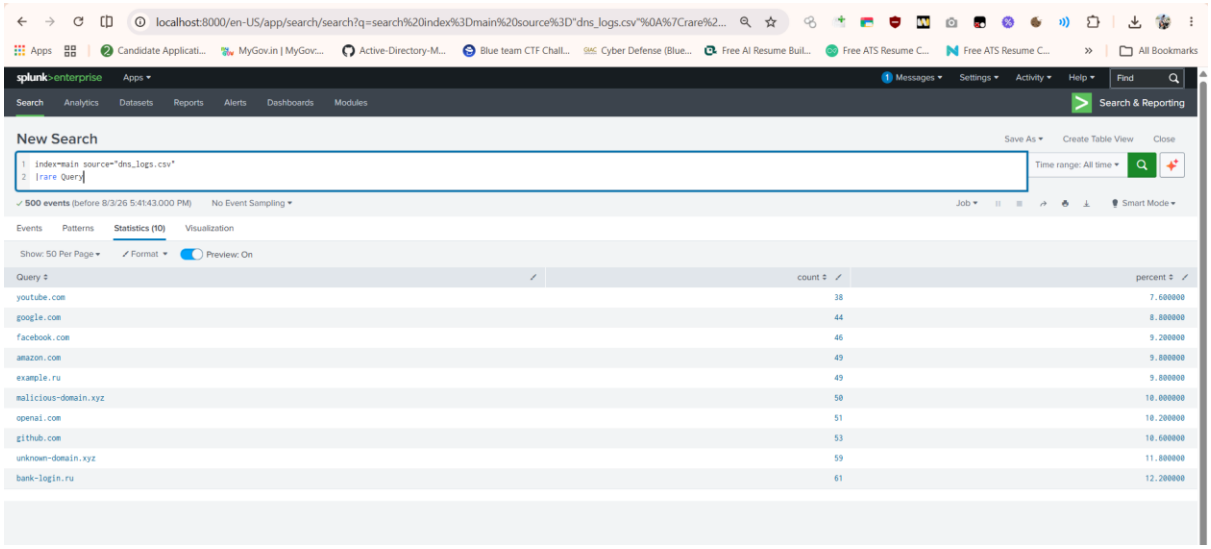

localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20source%3D"dns_logs.csv"%20%20Status%3D"...
splunk>enterprise
Search & Reporting
New Search
index=main source="dns_logs.csv" Status="NXDOMAIN"
109 events (before 8/3/26 5:28:45.000 PM)
Events (109)
Time
Event
8/3/26 12:04:45.192 PM
2026-08-03 12:04:45,192.168.1.29,8.8.8.8,unknown-domain.xyz,A,0.0.0.0,NXDOMAIN
host = abhiram source = dns_logs.csv sourcetype = csv
8/3/26 12:04:30.192 PM
2026-08-03 12:04:30,192.168.1.23,8.8.8.8,malicious-domain.xyz,A,0.0.0.0,NXDOMAIN
host = abhiram source = dns_logs.csv sourcetype = csv
8/3/26 12:04:15.192 PM
2026-08-03 12:04:15,192.168.1.39,8.8.8.8,unknown-domain.xyz,A,0.0.0.0,NXDOMAIN
host = abhiram source = dns_logs.csv sourcetype = csv
8/3/26 12:04:00.192 PM
2026-08-03 12:04:00,192.168.1.18,8.8.8.8,unknown-domain.xyz,A,0.0.0.0,NXDOMAIN
host = abhiram source = dns_logs.csv sourcetype = csv
8/3/26 12:02:30.192 PM
2026-08-03 12:02:30,192.168.1.26,8.8.8.8,malicious-domain.xyz,A,0.0.0.0,NXDOMAIN
host = abhiram source = dns_logs.csv sourcetype = csv
8/3/26 11:59:45.192 AM
2026-08-03 11:59:45,192.168.1.36,8.8.8.8,unknown-domain.xyz,A,0.0.0.0,NXDOMAIN
host = abhiram source = dns_logs.csv sourcetype = csv
8/3/26 11:59:00.192 AM
2026-08-03 11:59:00,192.168.1.28,8.8.8.8,unknown-domain.xyz,A,0.0.0.0,NXDOMAIN
host = abhiram source = dns_logs.csv sourcetype = csv

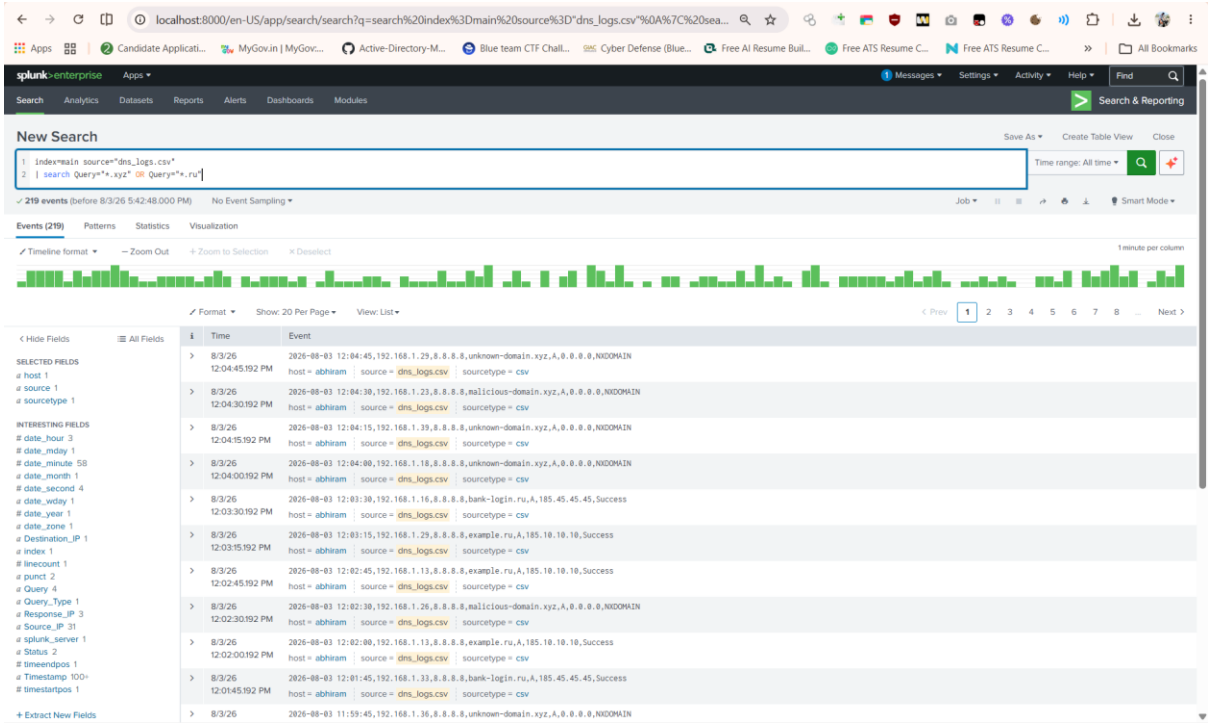

localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20source%3D"dns_logs.csv"%20%20Status%3D"S...
splunk>enterprise
Search & Reporting
New Search
index=main source="dns_logs.csv" Status="Success"
391 events (before 8/3/26 5:29:11.000 PM)
Events (391)
Time
Event
8/3/26 12:03:45.192 PM
2026-08-03 12:03:45,192.168.1.23,8.8.8.8,github.com,A,140.82.121.4,Success
host = abhiram source = dns_logs.csv sourcetype = csv
8/3/26 12:03:30.192 PM
2026-08-03 12:03:30,192.168.1.16,8.8.8.8,bank-login.ru,A,185.45.45.45,Success
host = abhiram source = dns_logs.csv sourcetype = csv
8/3/26 12:03:15.192 PM
2026-08-03 12:03:15,192.168.1.29,8.8.8.8,example.ru,A,185.10.10.10,Success
host = abhiram source = dns_logs.csv sourcetype = csv
8/3/26 12:03:00.192 PM
2026-08-03 12:03:00,192.168.1.38,8.8.8.8,github.com,A,140.82.121.4,Success
host = abhiram source = dns_logs.csv sourcetype = csv
8/3/26 12:02:45.192 PM
2026-08-03 12:02:45,192.168.1.13,8.8.8.8,example.ru,A,185.10.10.10,Success
host = abhiram source = dns_logs.csv sourcetype = csv
8/3/26 12:02:15.192 PM
2026-08-03 12:02:15,192.168.1.21,8.8.8.8,google.com,A,142.250.182.14,Success
host = abhiram source = dns_logs.csv sourcetype = csv
8/3/26 12:02:00.192 PM
2026-08-03 12:02:00,192.168.1.13,8.8.8.8,example.ru,A,185.10.10.10,Success
host = abhiram source = dns_logs.csv sourcetype = csv

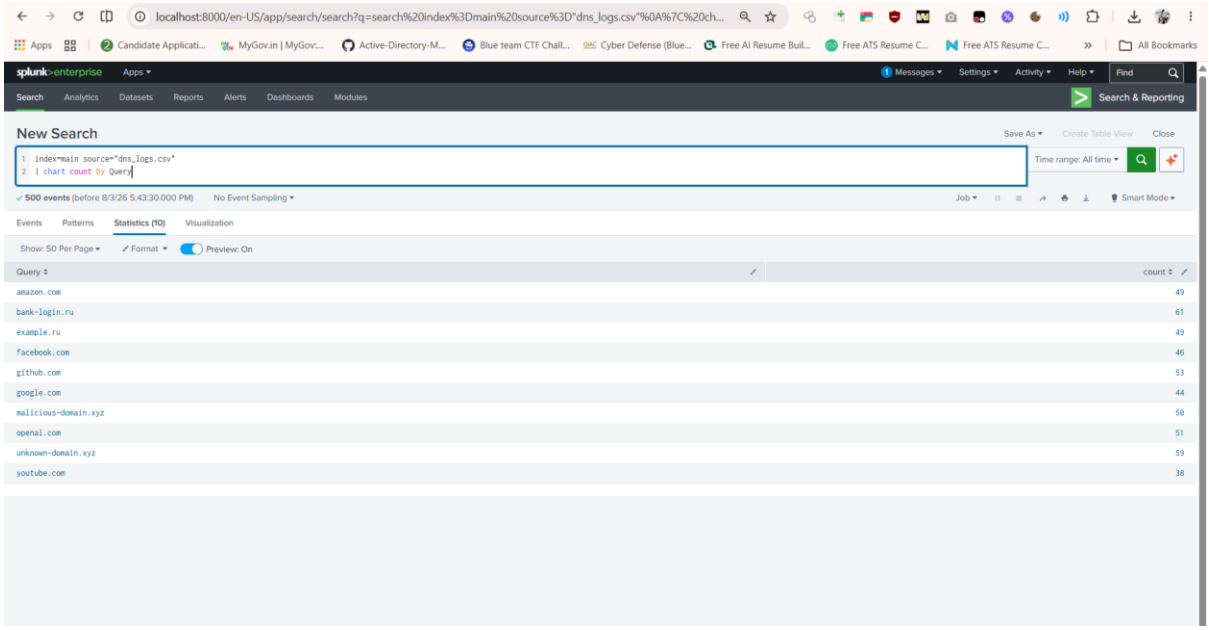

localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20source%3D"dns_security_logs.csv"%0A%...
splunk>enterprise
Apps
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Modules
Search & Reporting
New Search
Save As
Create Table View
Close
index=main source="dns_security_logs.csv"
| stats count by Source_IP
| where count>100
Time range: Last 24 hours
3,550 events (8/3/26 5:30:00.000 PM to 8/4/26 6:22:44.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (19)
Visualization
Show: 20 Per Page
Format
Preview: On
Source_IP
count
192.168.1.50 400
192.168.1.30 119
192.168.1.27 114
192.168.1.31 113
192.168.1.22 109
192.168.1.12 108
192.168.1.25 107
192.168.1.33 107
192.168.1.34 106
192.168.1.14 105
192.168.1.24 105
192.168.1.13 104
192.168.1.36 104
192.168.1.38 104

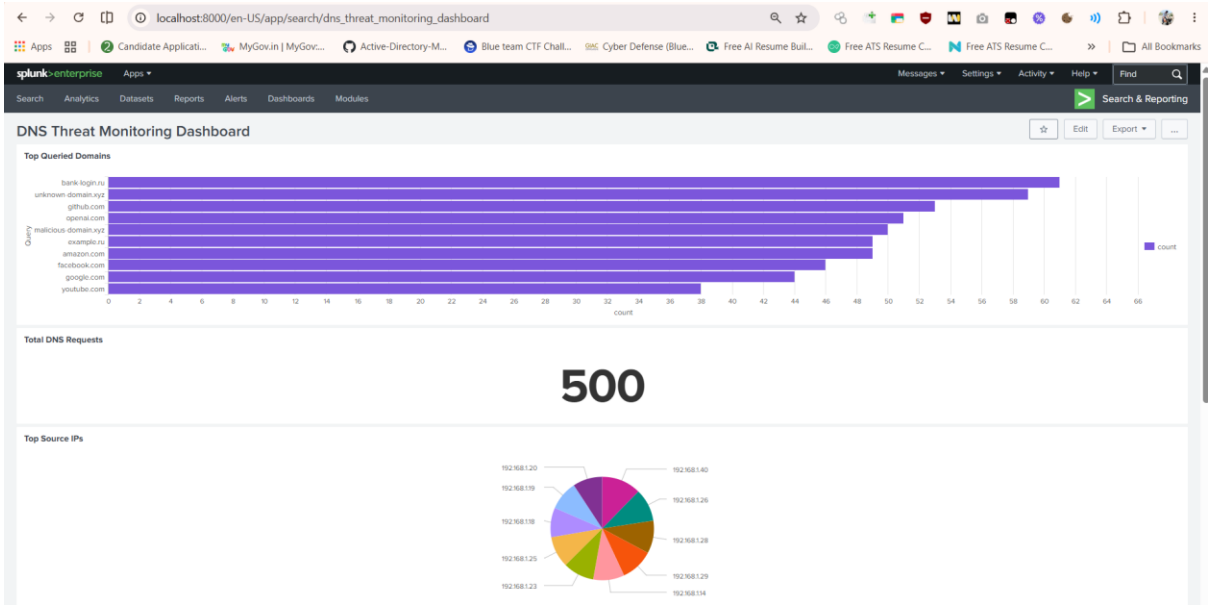

splunk>enterprise
Apps
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Modules
Search & Reporting
New Search
Save As
Create Table View
Close
index=main source="dns_logs.csv"
| eval length=len(Query)
| where length>50
Time range: All time
0 events (before 8/3/26 5:37:29.000 PM)
No Event Sampling
Job
Smart Mode
Events (0)
Patterns
Statistics
Visualization
No results found.


localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20source%3D"dns_logs.csv"%0A%7C%20rex...
splunk>enterprise
Search & Reporting
New Search
index=main source="dns_logs.csv"
| rex field=_raw "(?<Timestamp>[^,]+),(?<Source_IP>[^,]+),(?<Destination_IP>[^,]+),(?<Query>[^,]+),(?<Query_Type>[^,]+),(?<Response_IP>[^,]+),(?<Status>[^,]+)"
| eval length=len(Query)
| where length>15
| table Source_IP Query length
✓ 109 events (before 8/3/26 5:40:04.000 PM)
Events
Patterns
Statistics (109)
Visualization
Source_IP
Query
length
192.168.1.31 malicious-domain.xyz 20
192.168.1.23 unknown-domain.xyz 18
192.168.1.15 unknown-domain.xyz 18
192.168.1.35 malicious-domain.xyz 20
192.168.1.32 malicious-domain.xyz 20
192.168.1.11 unknown-domain.xyz 18
192.168.1.26 unknown-domain.xyz 18
192.168.1.13 malicious-domain.xyz 20
192.168.1.16 unknown-domain.xyz 18
192.168.1.20 unknown-domain.xyz 18
192.168.1.40 malicious-domain.xyz 20
192.168.1.21 unknown-domain.xyz 18
192.168.1.37 unknown-domain.xyz 18
192.168.1.20 malicious-domain.xyz 20
192.168.1.17 malicious-domain.xyz 20
192.168.1.40 unknown-domain.xyz 18
192.168.1.10 unknown-domain.xyz 18
192.168.1.16 unknown-domain.xyz 18
192.168.1.31 unknown-domain.xyz 18
192.168.1.37 unknown-domain.xyz 18


localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20source%3D"dns_logs.csv"%0A%7Crare%2...
splunk>enterprise
Search & Reporting
New Search
index=main source="dns_logs.csv"
|rare Query
✓ 500 events (before 8/3/26 5:41:43.000 PM)
Events
Patterns
Statistics (10)
Visualization
Query
count
percent
youtube.com 38 7.600000
google.com 44 8.800000
facebook.com 46 9.200000
amazon.com 49 9.800000
example.ru 49 9.800000
malicious-domain.xyz 50 10.000000
openai.com 51 10.200000
github.com 53 10.600000
unknown-domain.xyz 59 11.800000
bank-login.ru 61 12.200000


localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20source%3D"dns_logs.csv"%0A%7C%20sea...
splunk>enterprise
Search & Reporting
New Search
index=main source="dns_logs.csv"
| search Query="*.xyz" OR Query="*.ru"
219 events (before 8/3/26 5:42:48.000 PM)
Events (219)
Time
Event
2026-08-03 12:04:45,192.168.1.29,8.8.8.8,unknown-domain.xyz,A,0.0.0.0,NXDOMAIN
2026-08-03 12:04:30,192.168.1.23,8.8.8.8,malicious-domain.xyz,A,0.0.0.0,NXDOMAIN
2026-08-03 12:04:15,192.168.1.39,8.8.8.8,unknown-domain.xyz,A,0.0.0.0,NXDOMAIN
2026-08-03 12:04:00,192.168.1.18,8.8.8.8,unknown-domain.xyz,A,0.0.0.0,NXDOMAIN
2026-08-03 12:03:30,192.168.1.16,8.8.8.8,bank-login.ru,A,185.45.45.45,Success
2026-08-03 12:03:15,192.168.1.29,8.8.8.8,example.ru,A,185.10.10.10,Success
2026-08-03 12:02:45,192.168.1.13,8.8.8.8,example.ru,A,185.10.10.10,Success
2026-08-03 12:02:30,192.168.1.26,8.8.8.8,malicious-domain.xyz,A,0.0.0.0,NXDOMAIN
2026-08-03 12:02:00,192.168.1.13,8.8.8.8,example.ru,A,185.10.10.10,Success
2026-08-03 12:01:45,192.168.1.33,8.8.8.8,bank-login.ru,A,185.45.45.45,Success
2026-08-03 11:59:45,192.168.1.36,8.8.8.8,unknown-domain.xyz,A,0.0.0.0,NXDOMAIN


localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20source%3D"dns_logs.csv"%0A%7C%20ch...
splunk>enterprise
Search & Reporting
New Search
index=main source="dns_logs.csv"
| chart count by Query
500 events (before 8/3/26 5:43:30.000 PM)
Statistics (10)
Query
count
amazon.com 49
bank-login.ru 61
example.ru 49
facebook.com 46
github.com 53
google.com 44
malicious-domain.xyz 50
openai.com 51
unknown-domain.xyz 59
youtube.com 38

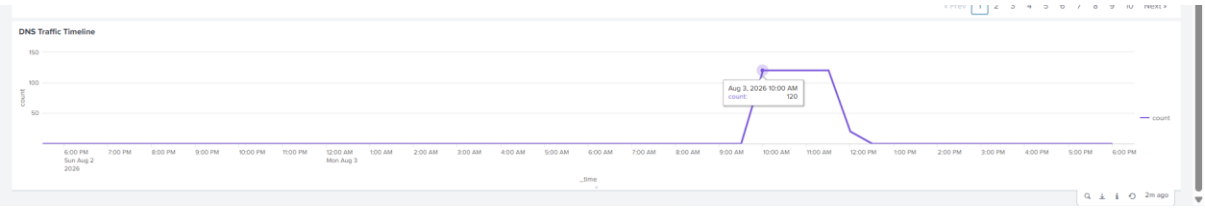


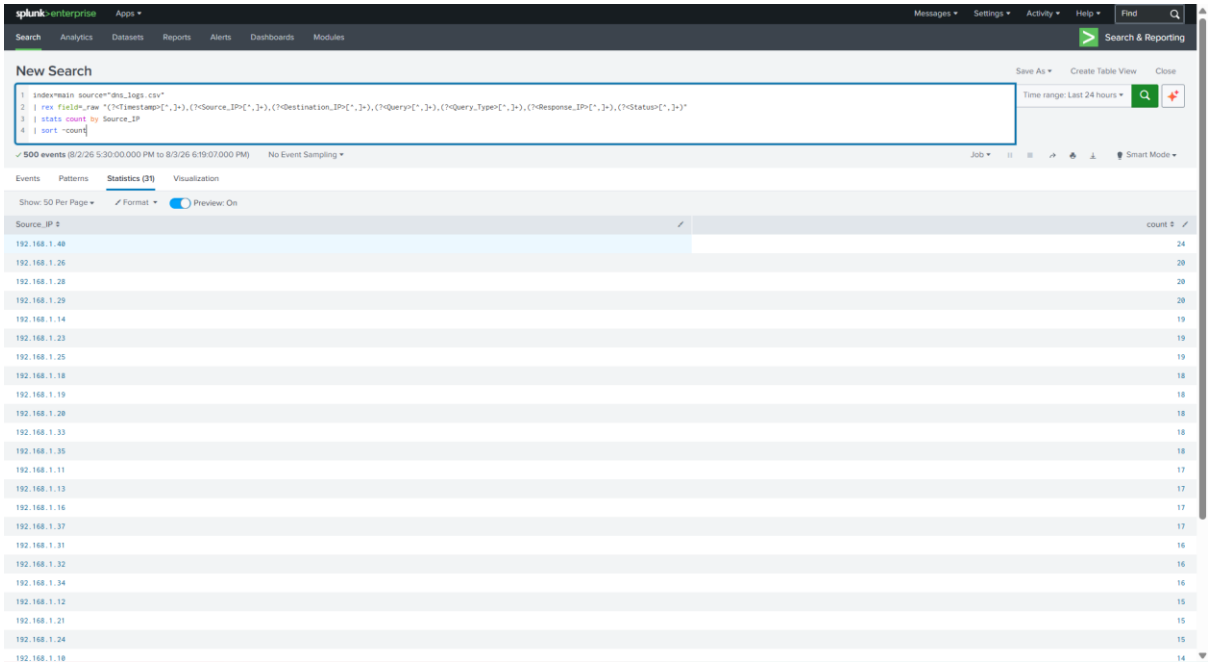
Failed DNS Queries

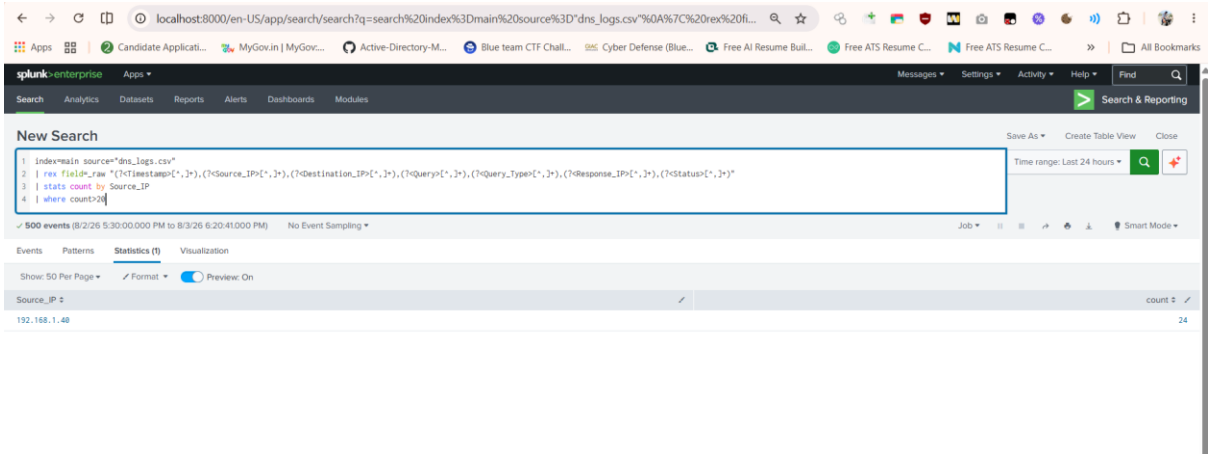
Timestamp	Source_IP	Query	Status
2026-08-03 10:29:00	192.168.1.31	malicious-domain.xyz	NXDOMAIN
2026-08-03 10:27:30	192.168.1.23	unknown-domain.xyz	NXDOMAIN
2026-08-03 10:27:15	192.168.1.15	unknown-domain.xyz	NXDOMAIN
2026-08-03 10:26:00	192.168.1.35	malicious-domain.xyz	NXDOMAIN
2026-08-03 10:22:15	192.168.1.32	malicious-domain.xyz	NXDOMAIN
2026-08-03 10:21:45	192.168.1.11	unknown-domain.xyz	NXDOMAIN
2026-08-03 10:19:15	192.168.1.26	unknown-domain.xyz	NXDOMAIN
2026-08-03 10:18:45	192.168.1.13	malicious-domain.xyz	NXDOMAIN
2026-08-03 10:17:45	192.168.1.16	unknown-domain.xyz	NXDOMAIN
2026-08-03 10:17:30	192.168.1.20	unknown-domain.xyz	NXDOMAIN

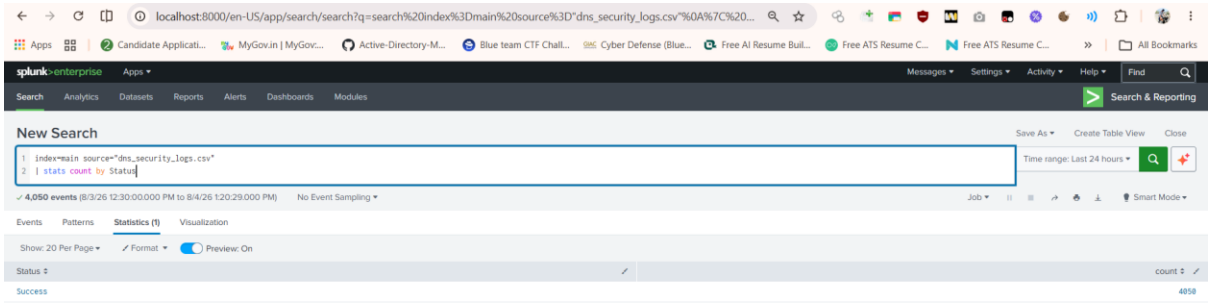
Suspicious Domain Detection

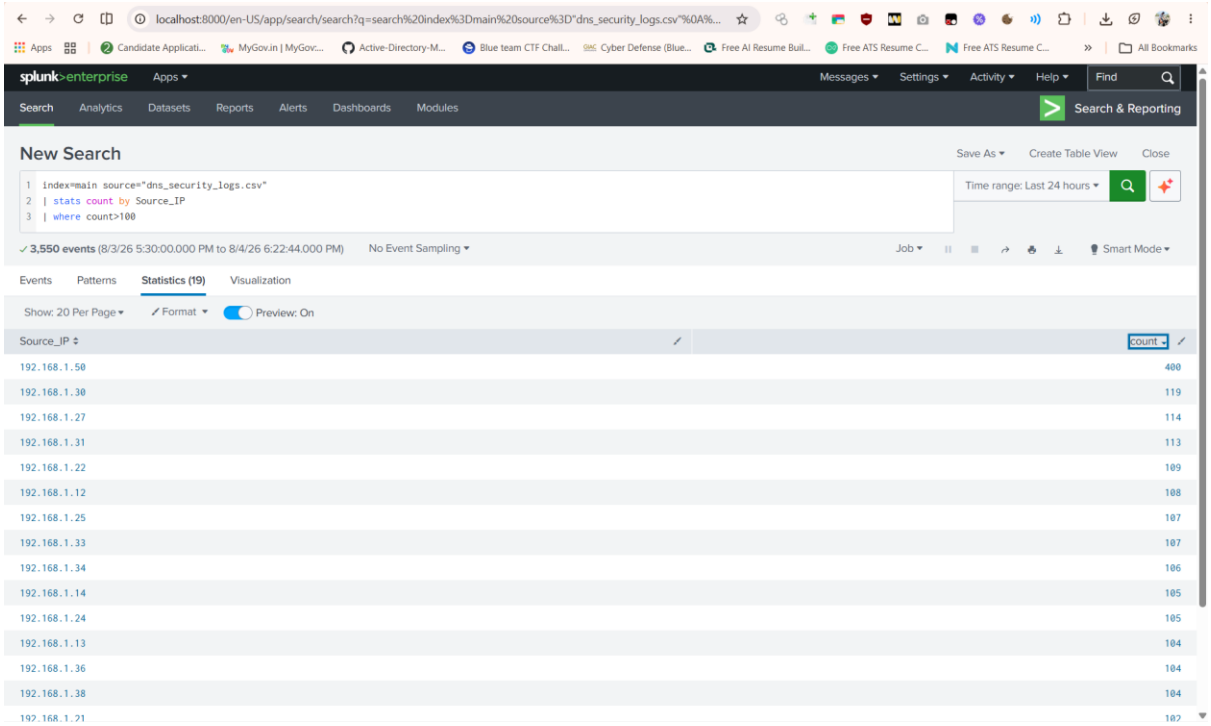
Timestamp	Source_IP	Query	Status
2026-08-03 10:30:45	192.168.1.21	bank-login.ru	Success
2026-08-03 10:30:15	192.168.1.16	example.ru	Success
2026-08-03 10:29:00	192.168.1.31	malicious-domain.xyz	NXDOMAIN
2026-08-03 10:28:45	192.168.1.12	example.ru	Success
2026-08-03 10:28:00	192.168.1.38	example.ru	Success
2026-08-03 10:27:30	192.168.1.23	unknown-domain.xyz	NXDOMAIN
2026-08-03 10:27:15	192.168.1.15	unknown-domain.xyz	NXDOMAIN
2026-08-03 10:26:30	192.168.1.34	example.ru	Success
2026-08-03 10:26:00	192.168.1.35	malicious-domain.xyz	NXDOMAIN
2026-08-03 10:25:30	192.168.1.23	example.ru	Success

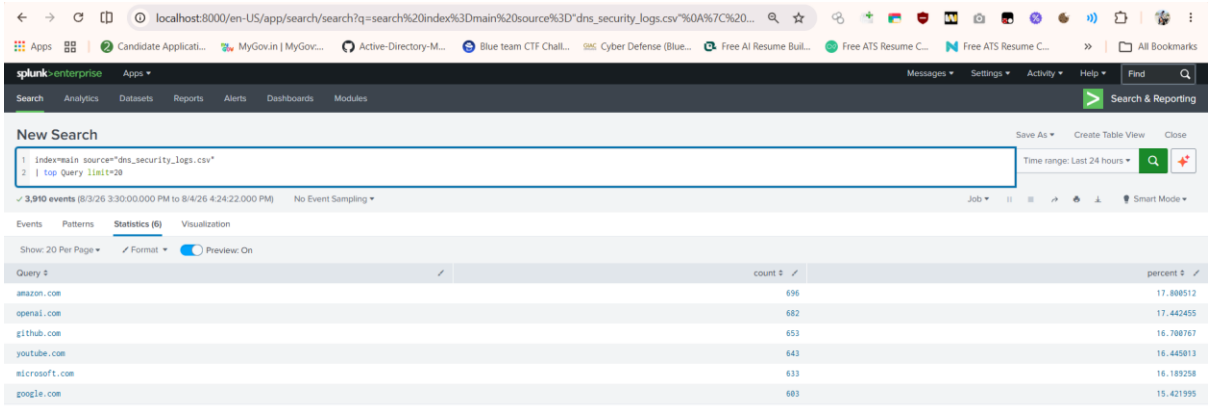


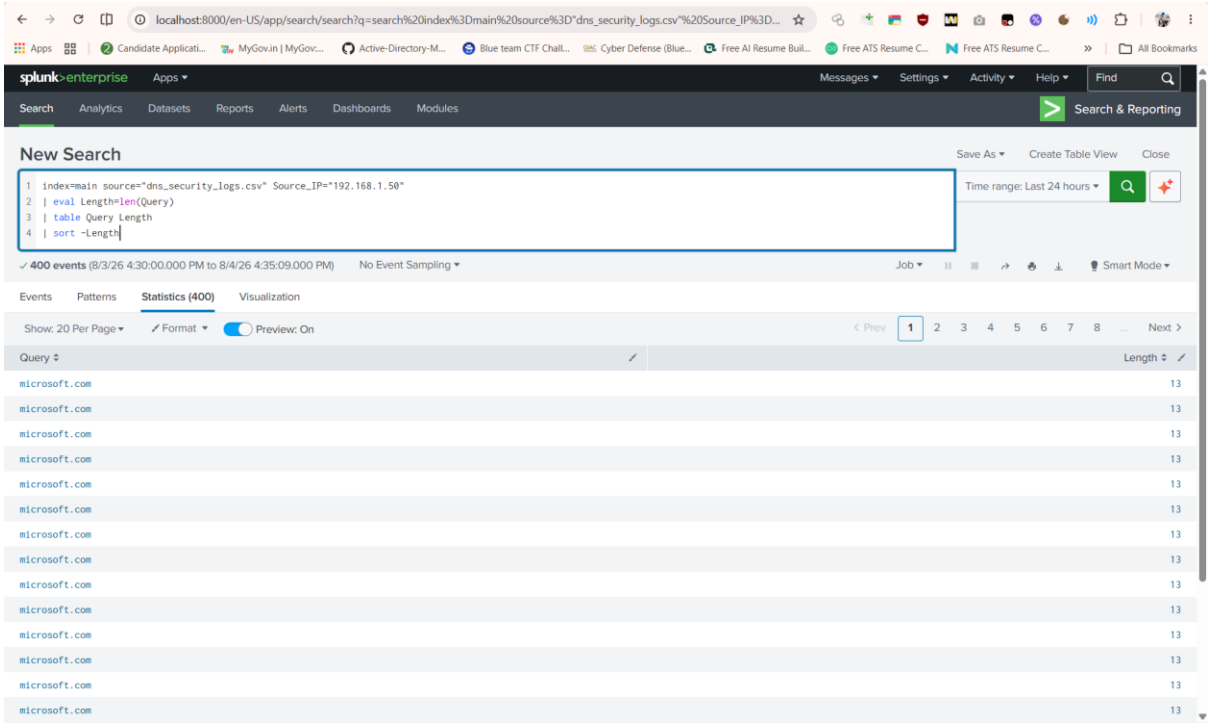

New Search
index=main source="dns_logs.csv"
| rex field=_raw "(?<Timestamp>[^,]+),(?<Source_IP>[^,]+),(?<Destination_IP>[^,]+),(?<Query>[^,]+),(?<Query_Type>[^,]+),(?<Response_IP>[^,]+),(?<Status>[^,]+)"
| stats count by Source_IP
| sort -count
✓ 500 events (8/2/26 5:30:00.000 PM to 8/3/26 6:19:07.000 PM)
Source_IP count
192.168.1.40 24
192.168.1.26 20
192.168.1.28 20
192.168.1.29 20
192.168.1.14 19
192.168.1.23 19
192.168.1.25 19
192.168.1.18 18
192.168.1.19 18
192.168.1.20 18
192.168.1.33 18
192.168.1.35 18
192.168.1.11 17
192.168.1.13 17
192.168.1.16 17
192.168.1.37 17
192.168.1.31 16
192.168.1.32 16
192.168.1.34 16
192.168.1.12 15
192.168.1.21 15
192.168.1.24 15
192.168.1.10 14

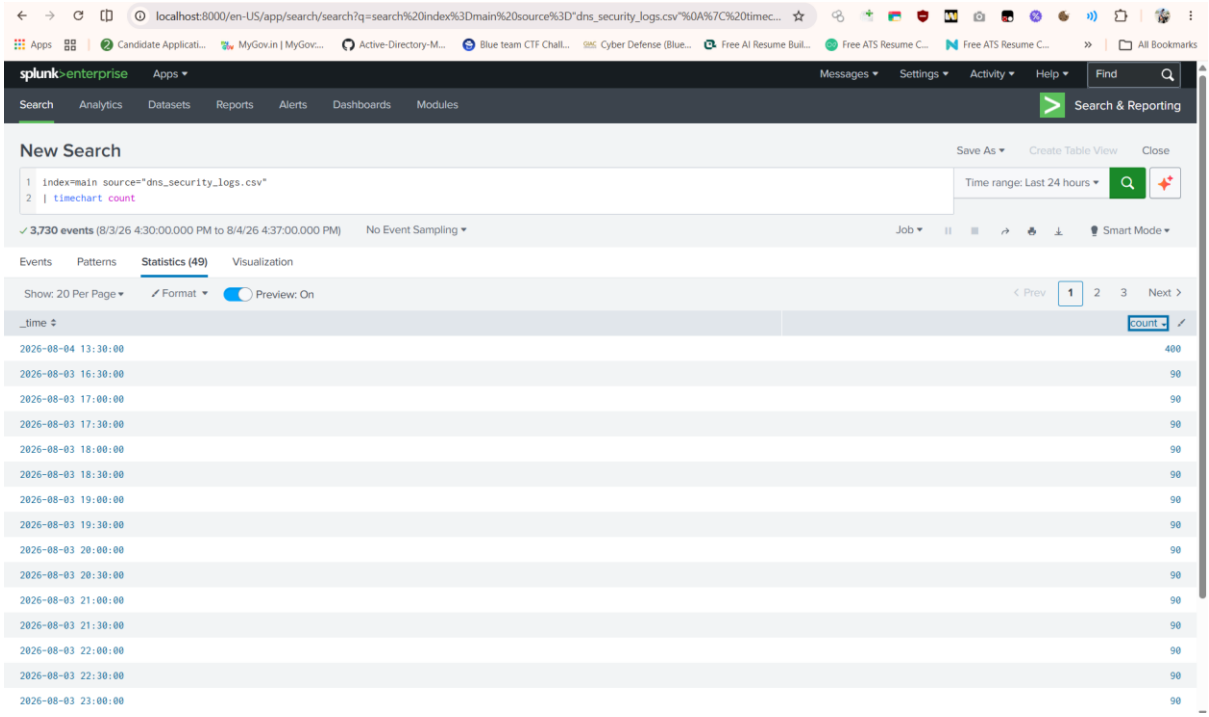

New Search
index=main source="dns_logs.csv"
| rex field=_raw "(?<Timestamp>[^,]+),(?<Source_IP>[^,]+),(?<Destination_IP>[^,]+),(?<Query>[^,]+),(?<Query_Type>[^,]+),(?<Response_IP>[^,]+),(?<Status>[^,]+)"
| stats count by Source_IP
| where count>20
✓ 500 events (8/2/26 5:30:00.000 PM to 8/3/26 6:20:41.000 PM)
Source_IP count
192.168.1.40 24


New Search
index=main source="dns_security_logs.csv"
| stats count by Status
✓ 4,050 events (8/3/26 12:30:00.000 PM to 8/4/26 1:20:29.000 PM)
Status count
Success 4050


localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20source%3D"dns_security_logs.csv"%0A%...
splunk>enterprise
Search & Reporting
New Search
index=main source="dns_security_logs.csv"
| stats count by Source_IP
| where count>100
3,550 events (8/3/26 5:30:00.000 PM to 8/4/26 6:22:44.000 PM)
Events Patterns Statistics (19) Visualization
Source_IP count
192.168.1.50 400
192.168.1.30 119
192.168.1.27 114
192.168.1.31 113
192.168.1.22 109
192.168.1.12 108
192.168.1.25 107
192.168.1.33 107
192.168.1.34 106
192.168.1.14 105
192.168.1.24 105
192.168.1.13 104
192.168.1.36 104
192.168.1.38 104


localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20source%3D"dns_security_logs.csv"%0A%7C%20...
splunk>enterprise
Search & Reporting
New Search
index=main source="dns_security_logs.csv"
| top Query limit=20
3,910 events (8/3/26 3:30:00.000 PM to 8/4/26 4:24:22.000 PM)
Events Patterns Statistics (6) Visualization
Query count percent
amazon.com 696 17.800512
openai.com 682 17.442455
github.com 653 16.700767
youtube.com 643 16.445013
microsoft.com 633 16.189258
google.com 603 15.421995


localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20source%3D"dns_security_logs.csv"%20Source_IP%3D...
splunk>enterprise
Search & Reporting
New Search
index=main source="dns_security_logs.csv" Source_IP="192.168.1.50"
| eval Length=len(Query)
| table Query Length
| sort -Length
Time range: Last 24 hours
400 events (8/3/26 4:30:00.000 PM to 8/4/26 4:35:09.000 PM)
No Event Sampling
Events
Patterns
Statistics (400)
Visualization
Show: 20 Per Page
Format
Preview: On
Query
Length
microsoft.com 13


localhost:8000/en-US/app/search/search?q=search%20index%3Dmain%20source%3D"dns_security_logs.csv"%0A%7C%20timec...
splunk>enterprise
Search & Reporting
New Search
index=main source="dns_security_logs.csv"
| timechart count
Time range: Last 24 hours
3,730 events (8/3/26 4:30:00.000 PM to 8/4/26 4:37:00.000 PM)
No Event Sampling
Events
Patterns
Statistics (49)
Visualization
Show: 20 Per Page
Format
Preview: On
_time
count
2026-08-04 13:30:00 400
2026-08-03 16:30:00 90
2026-08-03 17:00:00 90
2026-08-03 17:30:00 90
2026-08-03 18:00:00 90
2026-08-03 18:30:00 90
2026-08-03 19:00:00 90
2026-08-03 19:30:00 90
2026-08-03 20:00:00 90
2026-08-03 20:30:00 90
2026-08-03 21:00:00 90
2026-08-03 21:30:00 90
2026-08-03 22:00:00 90
2026-08-03 22:30:00 90
2026-08-03 23:00:00 90