SOC Internship Project Plan (Splunk)

1. Project Title

"Security Event Monitoring and Threat Detection Using Splunk"

2. Datasets

You need logs to simulate a real SOC environment. You can use:

- **botsv1-attack-only.tgz (135MB)** → lightweight, contains attack logs (recommended for your system).
- (Optional later) **botsv1_data_set.tgz (6.1GB)** → full dataset with normal + attack traffic.

You can also extract smaller datasets for practice (from Malware-Traffic-Analysis.net, Kaggle, etc.).

3. Projects / Use Cases

Project 1: Phishing Email Detection

- **Dataset**: Email logs (from BOTS v1 or sample CSV).
- **Goal**: Detect phishing attempts based on suspicious senders, file attachments, or domains.
- **Example Query**:
- index=email_logs ("exe" OR "zip" OR "scr") OR sender_domain!="trusted.com"
- **Deliverable**: Dashboard showing flagged phishing emails.

Project 2: DNS Traffic Monitoring

- **Dataset**: DNS logs (2014-11-16 PCAP → extract DNS queries, or use BOTS DNS logs).
- **Goal**: Detect failed lookups and suspicious domain

Project goal: build SOC-style detections and dashboards for phishing, DNS anomalies, malware beaconing, brute-force logins and threat-intel enrichment using logs uploaded to index=main.

Important general notes before running queries

- **Time range:** Set Splunk time range to **All time** or appropriate span that contains your CSV events (top-right menu). Many sample files use older timestamps.
- **Index:** All queries below target index=main since your data is there.
- **Check field names:** If a query returns zero results, run index=main | head 20 and expand an event to confirm exact field names.

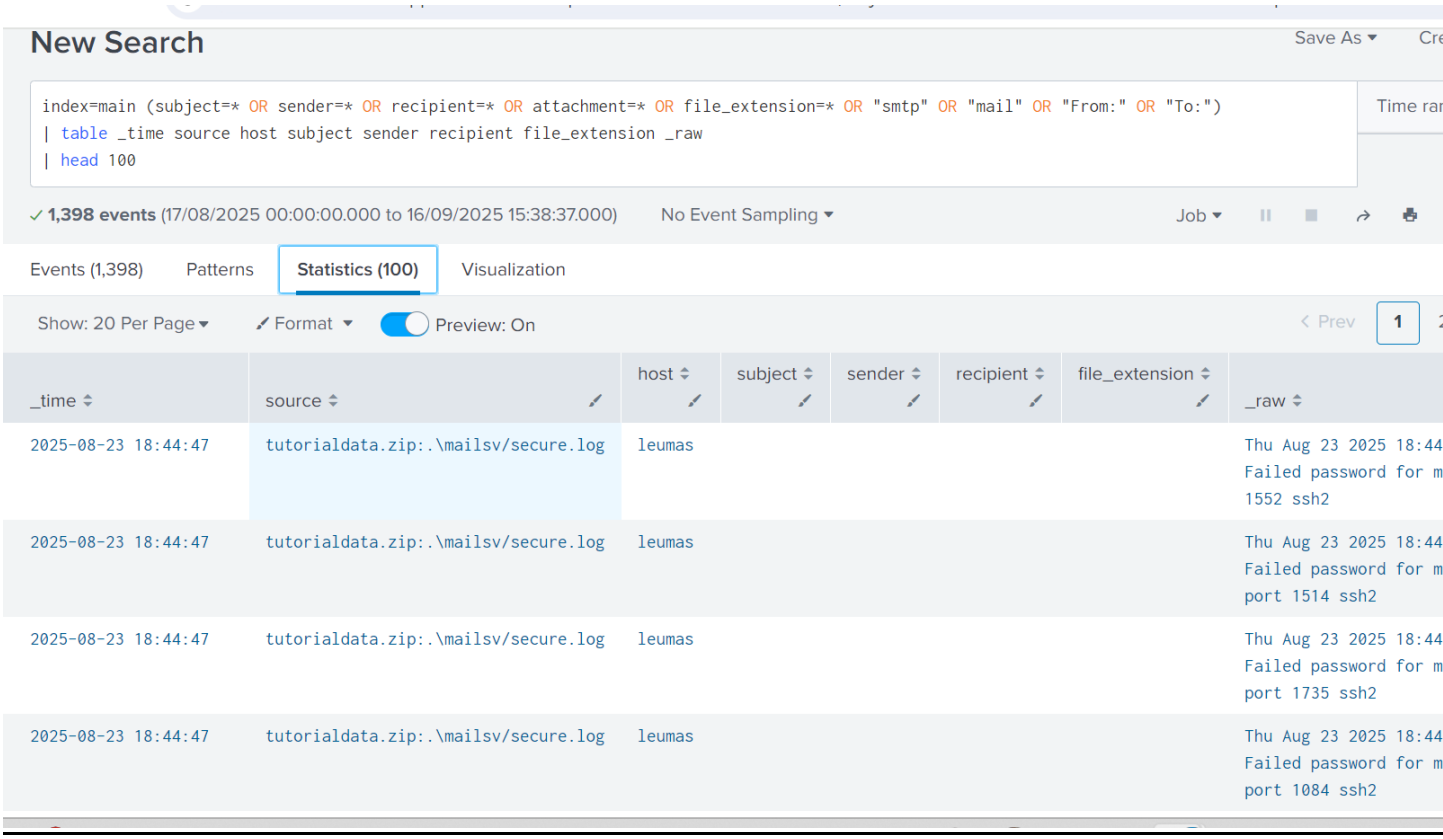
- **Search performance:** Use source="filename.csv" to limit to a file when testing to speed searches (e.g., index=main source="brute_force_attack.csv").
- **Screenshots:** For submission, capture both the query and its result table or chart.

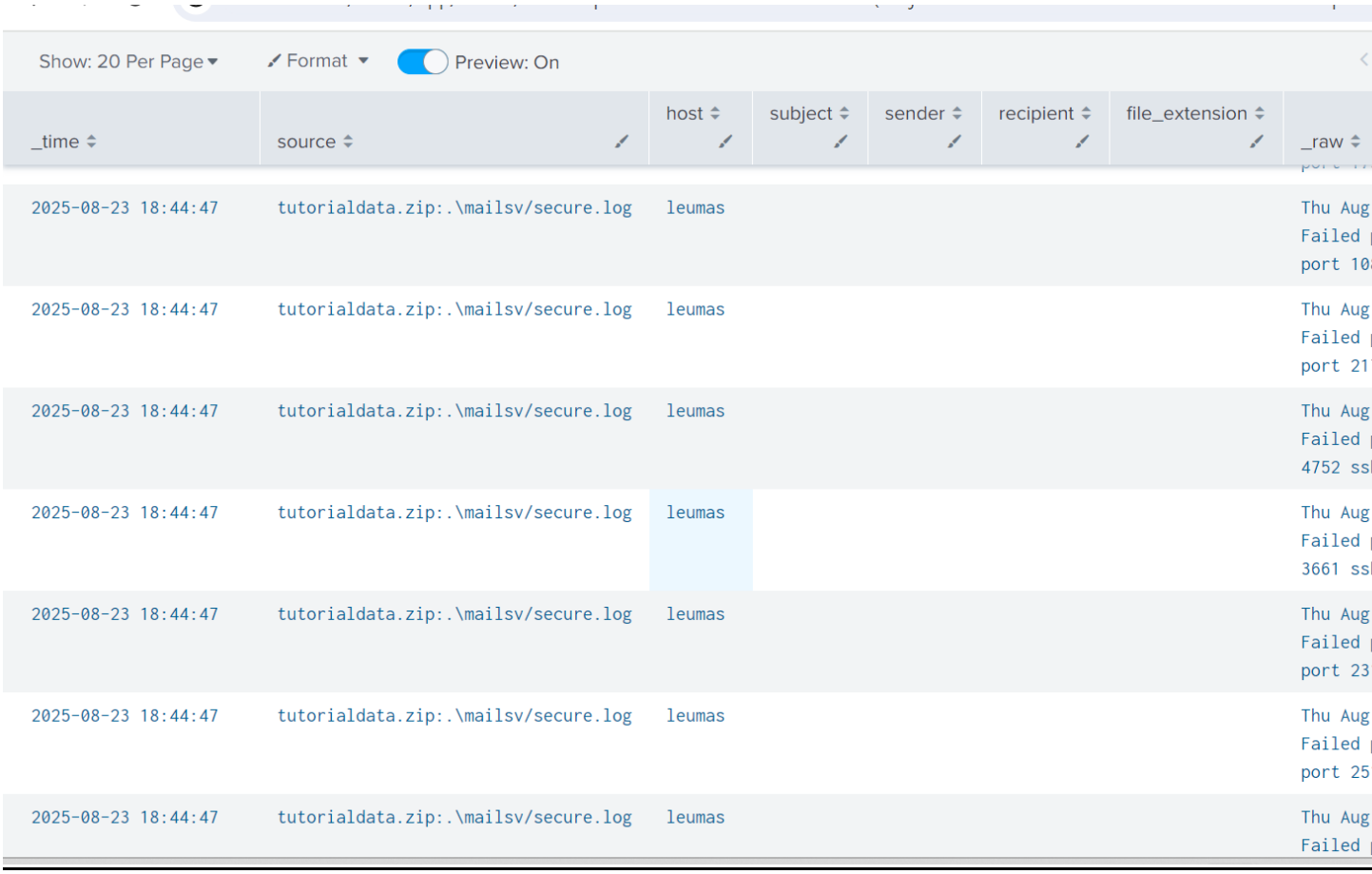
1) Phishing Email Detection

Detect suspicious attachments or emails from external domains:

Now search with:

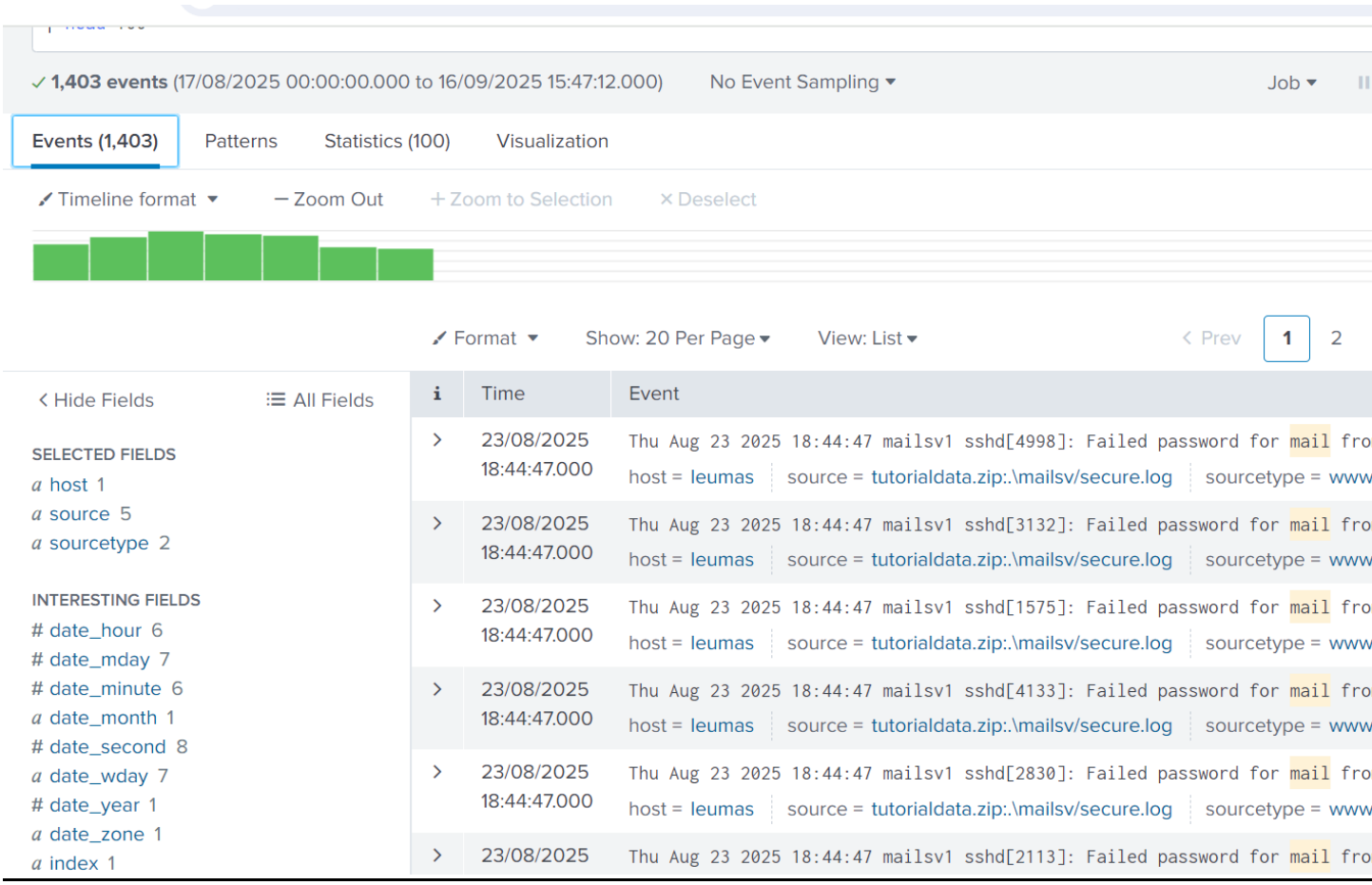
```
index=main (subject=* OR sender=* OR recipient=* OR attachment=* OR file_extension=* OR "smtp" OR "mail" OR "From:" OR "To:")
| table _time sender recipient subject attachment file_extension
| head 100
```

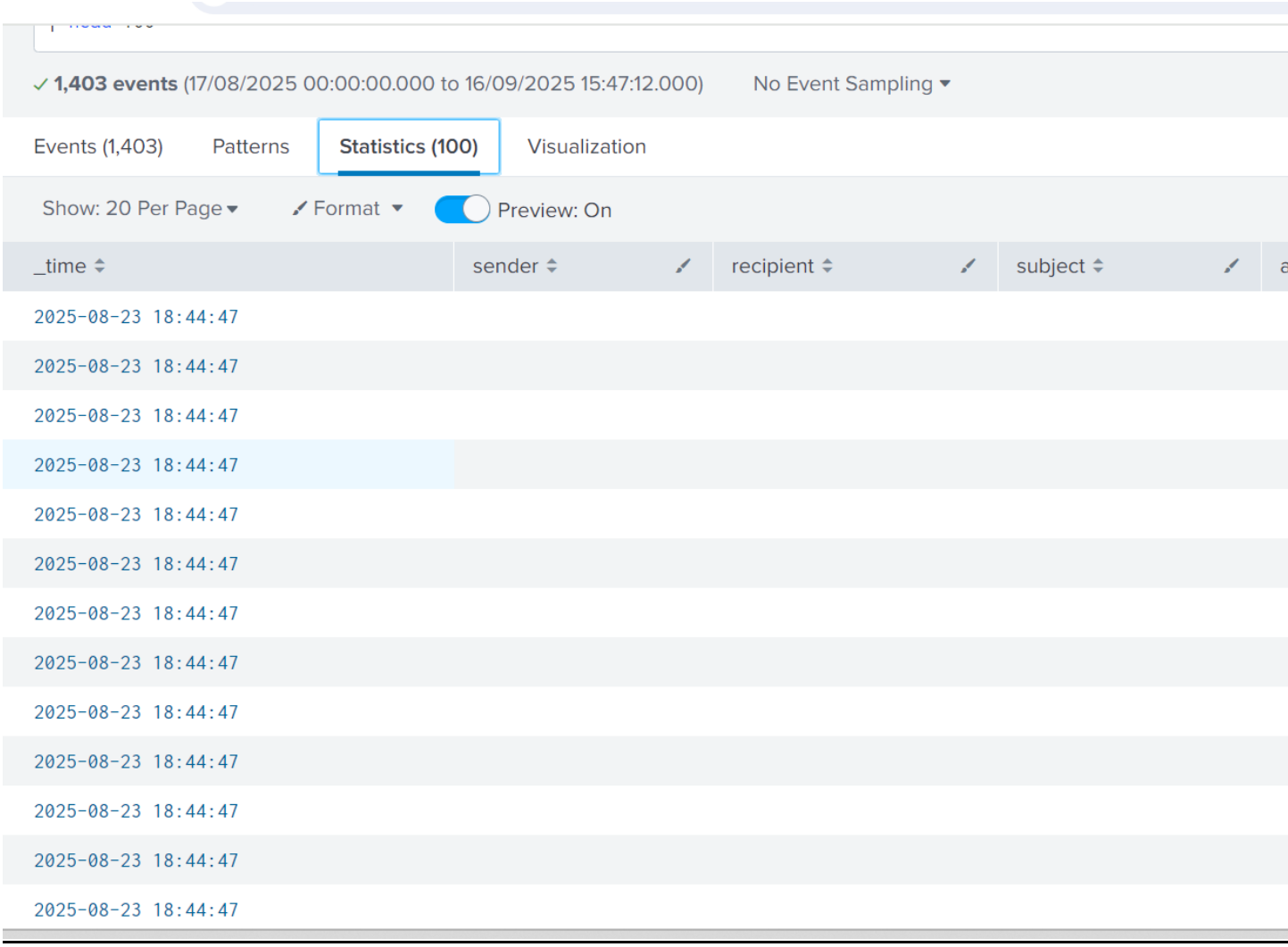

New Search
Save As
index=main (subject=* OR sender=* OR recipient=* OR attachment=* OR file_extension=* OR "smtp" OR "mail" OR "From:" OR "To:")
| table _time source host subject sender recipient file_extension _raw
| head 100
Time ran
1,398 events (17/08/2025 00:00:00.000 to 16/09/2025 15:38:37.000)
No Event Sampling
Job
Events (1,398)
Patterns
Statistics (100)
Visualization
Show: 20 Per Page
Format
Preview: On
Prev
1
_time
source
host
subject
sender
recipient
file_extension
_raw
2025-08-23 18:44:47
tutorialdata.zip:.\mailsv/secure.log
leumas
Thu Aug 23 2025 18:44
Failed password for m
1552 ssh2
2025-08-23 18:44:47
tutorialdata.zip:.\mailsv/secure.log
leumas
Thu Aug 23 2025 18:44
Failed password for m
port 1514 ssh2
2025-08-23 18:44:47
tutorialdata.zip:.\mailsv/secure.log
leumas
Thu Aug 23 2025 18:44
Failed password for m
port 1735 ssh2
2025-08-23 18:44:47
tutorialdata.zip:.\mailsv/secure.log
leumas
Thu Aug 23 2025 18:44
Failed password for m
port 1084 ssh2



Show: 20 Per Page | Format | Preview: On

_time	source	host	subject	sender	recipient	file_extension	_raw
2025-08-23 18:44:47	tutorialdata.zip:.\mailsv/secure.log	leumas					Thu Aug Failed port 10
2025-08-23 18:44:47	tutorialdata.zip:.\mailsv/secure.log	leumas					Thu Aug Failed port 21
2025-08-23 18:44:47	tutorialdata.zip:.\mailsv/secure.log	leumas					Thu Aug Failed 4752 ss
2025-08-23 18:44:47	tutorialdata.zip:.\mailsv/secure.log	leumas					Thu Aug Failed 3661 ss
2025-08-23 18:44:47	tutorialdata.zip:.\mailsv/secure.log	leumas					Thu Aug Failed port 23
2025-08-23 18:44:47	tutorialdata.zip:.\mailsv/secure.log	leumas					Thu Aug Failed port 25
2025-08-23 18:44:47	tutorialdata.zip:.\mailsv/secure.log	leumas					Thu Aug Failed


✓ 1,403 events (17/08/2025 00:00:00.000 to 16/09/2025 15:47:12.000)
No Event Sampling
Job
Events (1,403)
Patterns
Statistics (100)
Visualization
Timeline format
– Zoom Out
+ Zoom to Selection
× Deselect
Format
Show: 20 Per Page
View: List
Prev
1
2
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 5
a sourcetype 2
INTERESTING FIELDS
date_hour 6
date_mday 7
date_minute 6
a date_month 1
date_second 8
a date_wday 7
date_year 1
a date_zone 1
a index 1
Time
Event
23/08/2025 18:44:47.000
Thu Aug 23 2025 18:44:47 mailsv1 sshd[4998]: Failed password for mail fro
host = leumas source = tutorialdata.zip:.\mailsv\secure.log sourcetype = www
23/08/2025 18:44:47.000
Thu Aug 23 2025 18:44:47 mailsv1 sshd[3132]: Failed password for mail fro
host = leumas source = tutorialdata.zip:.\mailsv\secure.log sourcetype = www
23/08/2025 18:44:47.000
Thu Aug 23 2025 18:44:47 mailsv1 sshd[1575]: Failed password for mail fro
host = leumas source = tutorialdata.zip:.\mailsv\secure.log sourcetype = www
23/08/2025 18:44:47.000
Thu Aug 23 2025 18:44:47 mailsv1 sshd[4133]: Failed password for mail fro
host = leumas source = tutorialdata.zip:.\mailsv\secure.log sourcetype = www
23/08/2025 18:44:47.000
Thu Aug 23 2025 18:44:47 mailsv1 sshd[2830]: Failed password for mail fro
host = leumas source = tutorialdata.zip:.\mailsv\secure.log sourcetype = www
23/08/2025
Thu Aug 23 2025 18:44:47 mailsv1 sshd[2113]: Failed password for mail fro



Purpose

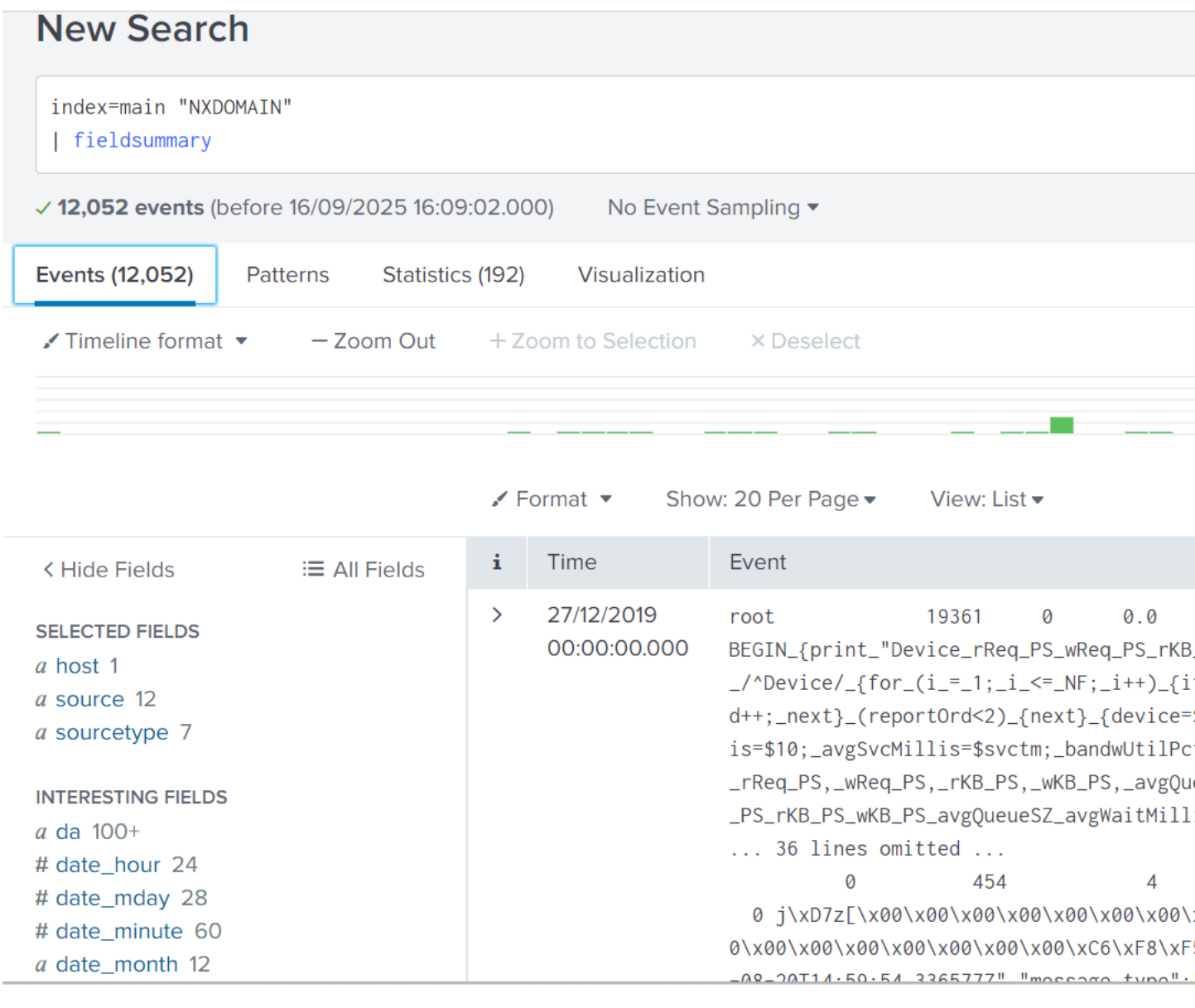
To filter and display email-related fields (subject, sender, recipient, attachment, file_extension) or common email keywords (smtp, mail, From:, To:) from the **main** index and limit the output to the first 100 events for review.

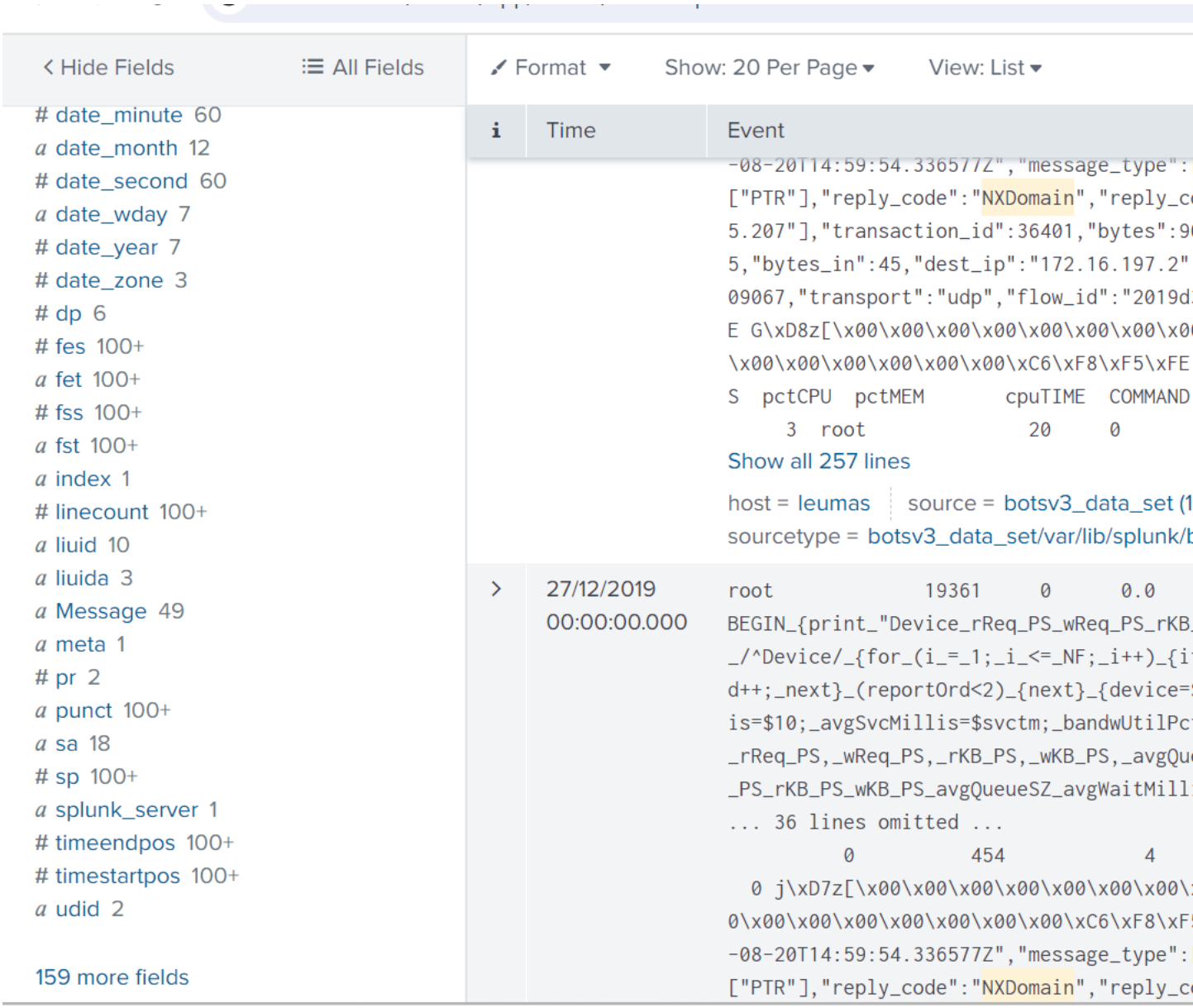
What this does:

1. **index=main** – Searches within the main index.
2. *(subject= OR sender=* OR recipient=* …)** – Filters for events containing any of these fields or keywords related to email (e.g., smtp, mail).
3. **| table …** – Displays only _time, sender, recipient, subject, attachment, and file_extension fields.
4. **| head 100** – Limits results to the first 100 events.

2) DNS Traffic Monitoring

Failed DNS lookups (NXDOMAIN):


New Search
index=main "NXDOMAIN"
| fieldsummary
✓ 12,052 events (before 16/09/2025 16:09:02.000)
No Event Sampling
Events (12,052)
Patterns
Statistics (192)
Visualization
Timeline format
– Zoom Out
+ Zoom to Selection
× Deselect
Format
Show: 20 Per Page
View: List
< Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 12
a sourcetype 7
INTERESTING FIELDS
a da 100+
date_hour 24
date_mday 28
date_minute 60
a date_month 12
Time
Event
27/12/2019 00:00:00.000
root 19361 0 0.0
BEGIN_{print_"Device_rReq_PS_wReq_PS_rKB
_/^Device/_{for_(i_=_1;_i_<=_NF;_i++)_{i
d++;_next}_(reportOrd<2)_{next}_{device=
is=$10;_avgSvcMillis=$svctm;_bandwUtilPc
_rReq_PS,_wReq_PS,_rKB_PS,_wKB_PS,_avgQu
_PS_rKB_PS_wKB_PS_avgQueueSZ_avgWaitMill
... 36 lines omitted ...
0 454 4
0 j\xD7z[\x00\x00\x00\x00\x00\x00\x00\
0\x00\x00\x00\x00\x00\x00\xC6\xF8\xF


Hide Fields
All Fields
Format
Show: 20 Per Page
View: List
date_minute 60
a date_month 12
date_second 60
a date_wday 7
date_year 7
date_zone 3
dp 6
fes 100+
a fet 100+
fss 100+
a fst 100+
a index 1
linecount 100+
a liuid 10
a liuida 3
a Message 49
a meta 1
pr 2
a punct 100+
a sa 18
sp 100+
a splunk_server 1
timeendpos 100+
timestartpos 100+
a udid 2
159 more fields
Time
Event
["PTR"],"reply_code":"NXDomain",
5,"bytes_in":45,"dest_ip":"172.16.197.2"
S pctCPU pctMEM cpuTIME COMMAND
3 root 20 0
Show all 257 lines
host = leumas
source = botsv3_data_set (1
sourcetype = botsv3_data_set/var/lib/splunk/b
27/12/2019
00:00:00.000
root 19361 0 0.0
BEGIN_{print_"Device_rReq_PS_wReq_PS_rKB
... 36 lines omitted ...
0 454 4
["PTR"],"reply_code":"NXDomain",

New Search

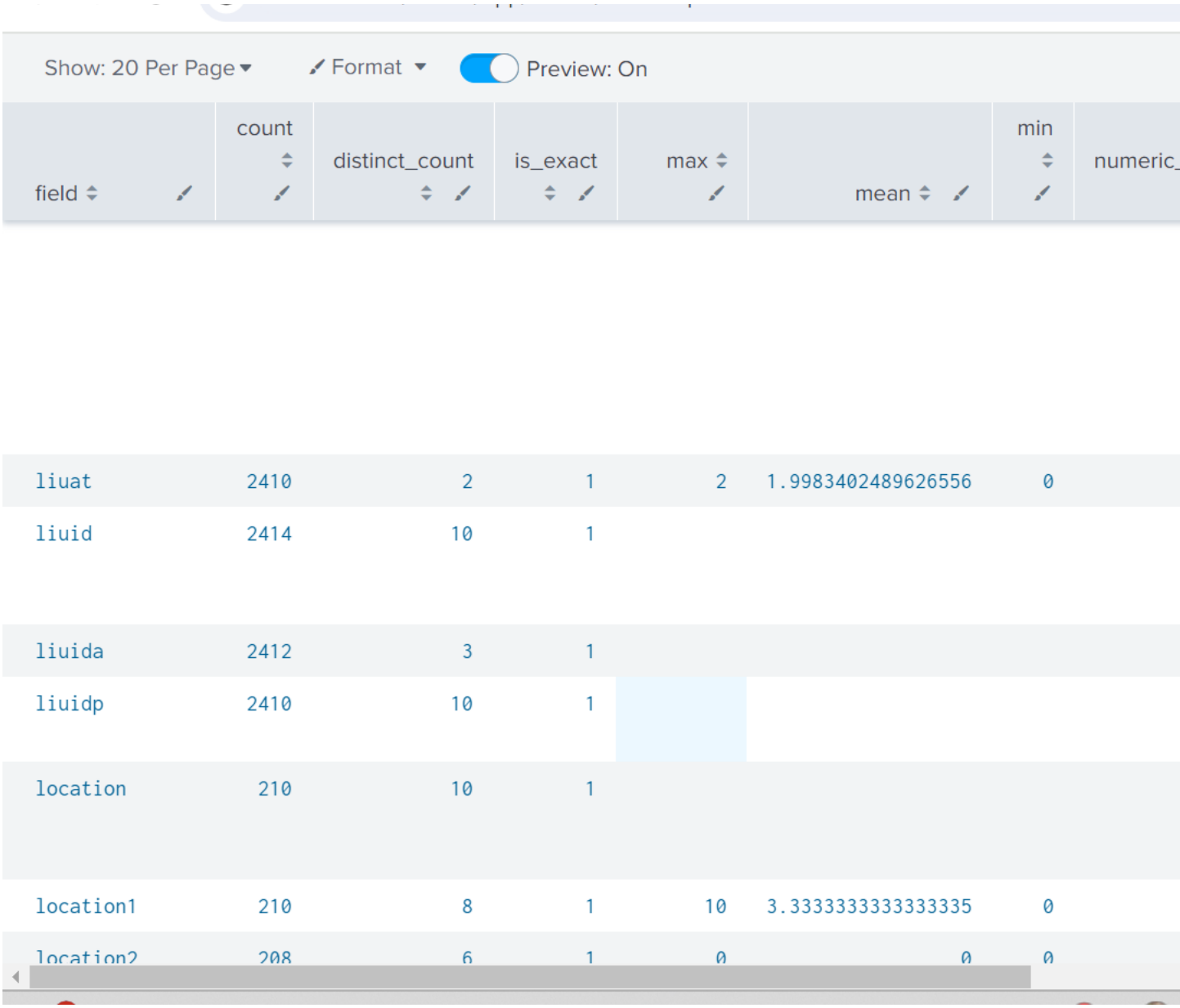
```
index=main "NXDOMAIN"
| fieldsummary
```

✓ **12,052 events** (before 16/09/2025 16:09:02.000) No Event Sampling

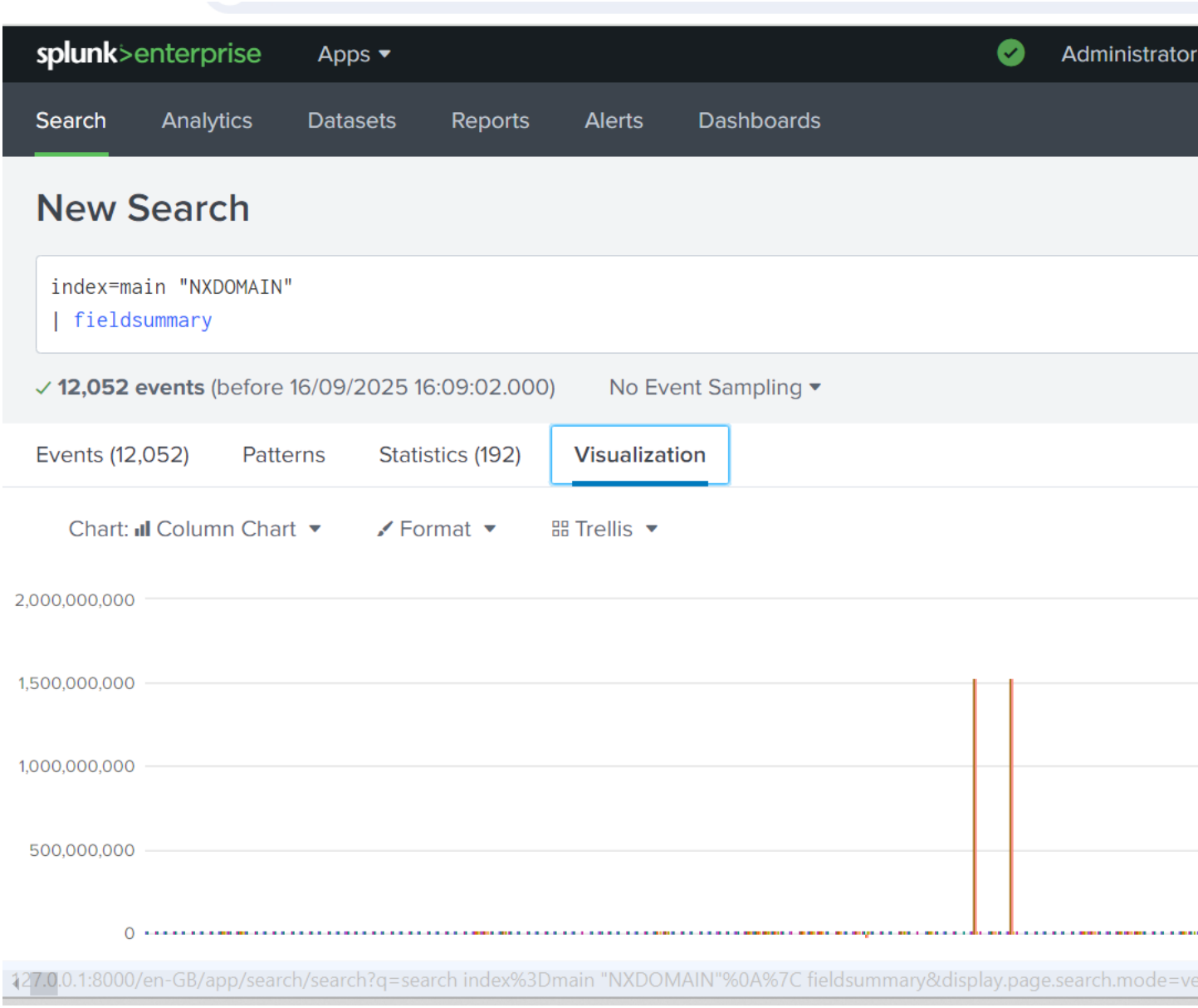
Events (12,052) Patterns **Statistics (192)** Visualization

Show: 20 Per Page Format Preview: On

field	count	distinct_count	is_exact	max	mean	min	nu
ApplicationDisplayName	2	1	1				
ApplicationId	2	1	1				
C	1066	4	1				
CN	1058	25	1				
ClientIP	4	2	1				
ComputerName	1090	13	1				
CorrelationId	2	1	1				



field	count	distinct_count	is_exact	max	mean	min	numeric_
liuat	2410	2	1	2	1.9983402489626556	0	
liuid	2414	10	1				
liuida	2412	3	1				
liuidp	2410	10	1				
location	210	10	1				
location1	210	8	1	10	3.3333333333333335	0	
location2	208	6	1	0	0	0	



Purpose

- To **discover and understand the available fields** in events containing "NXDOMAIN" in the main index.
- NXDOMAIN is a DNS response code meaning **"Non-Existent Domain."** This is often used to identify DNS lookup failures or potential suspicious activity like DNS tunneling or misconfigured hosts.

How It Works

1. **index=main "NXDOMAIN"**
    - Searches the **main** index for events containing the keyword NXDOMAIN.

- This filters DNS-related events that failed resolution.

2. **| fieldsummary**
   - Analyzes all returned events and produces a **summary of extracted fields**.
   - Shows:
     - **count** – Number of times the field appears.
     - **distinct_count** – Number of unique values.
     - **is_exact** – Indicates if the values are exact.
     - **min, max, mean** – Statistical summaries for numeric fields.
     - **values** – A preview of common field values.

Top Queried Domains

Query

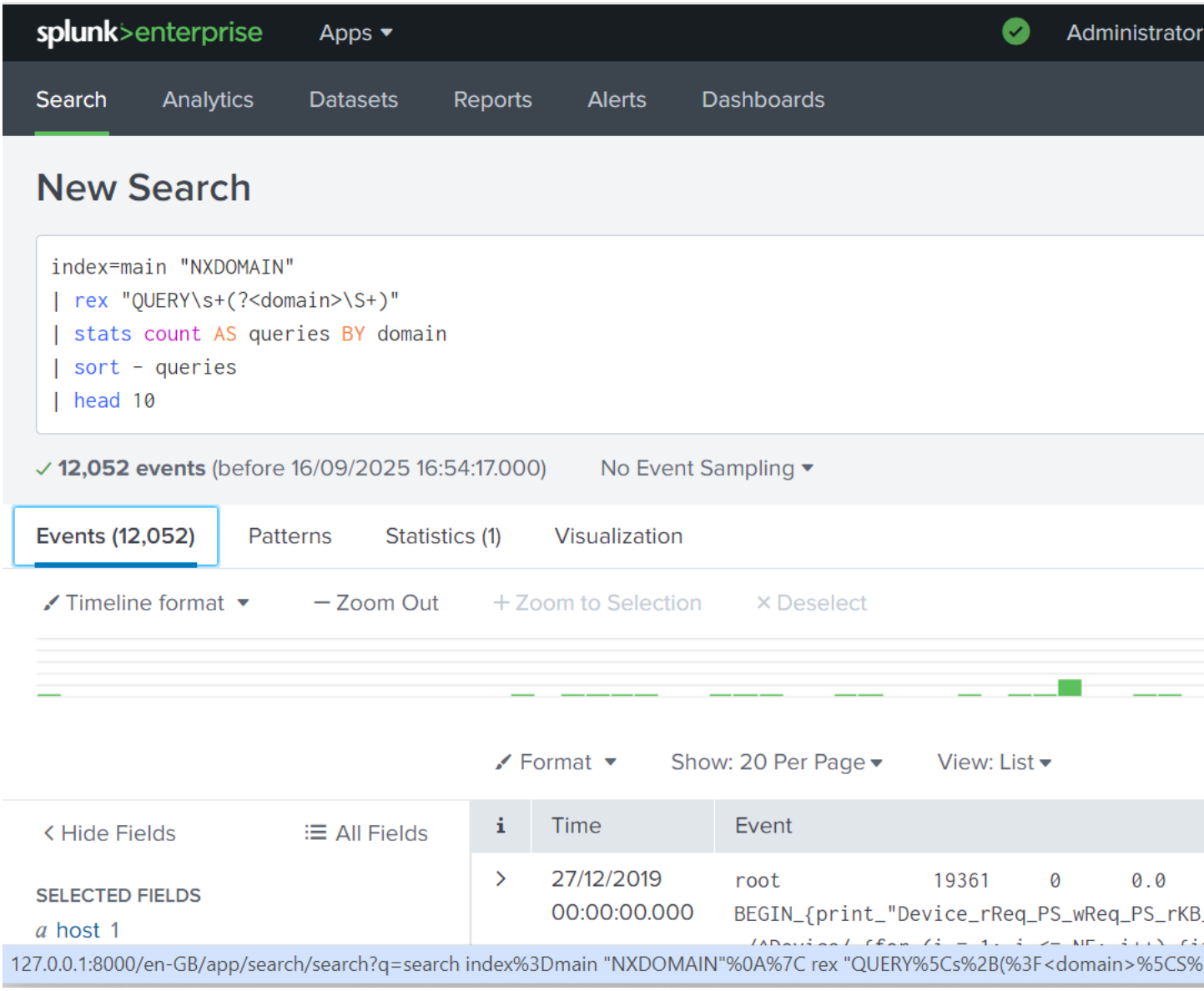
index=main "NXDOMAIN"

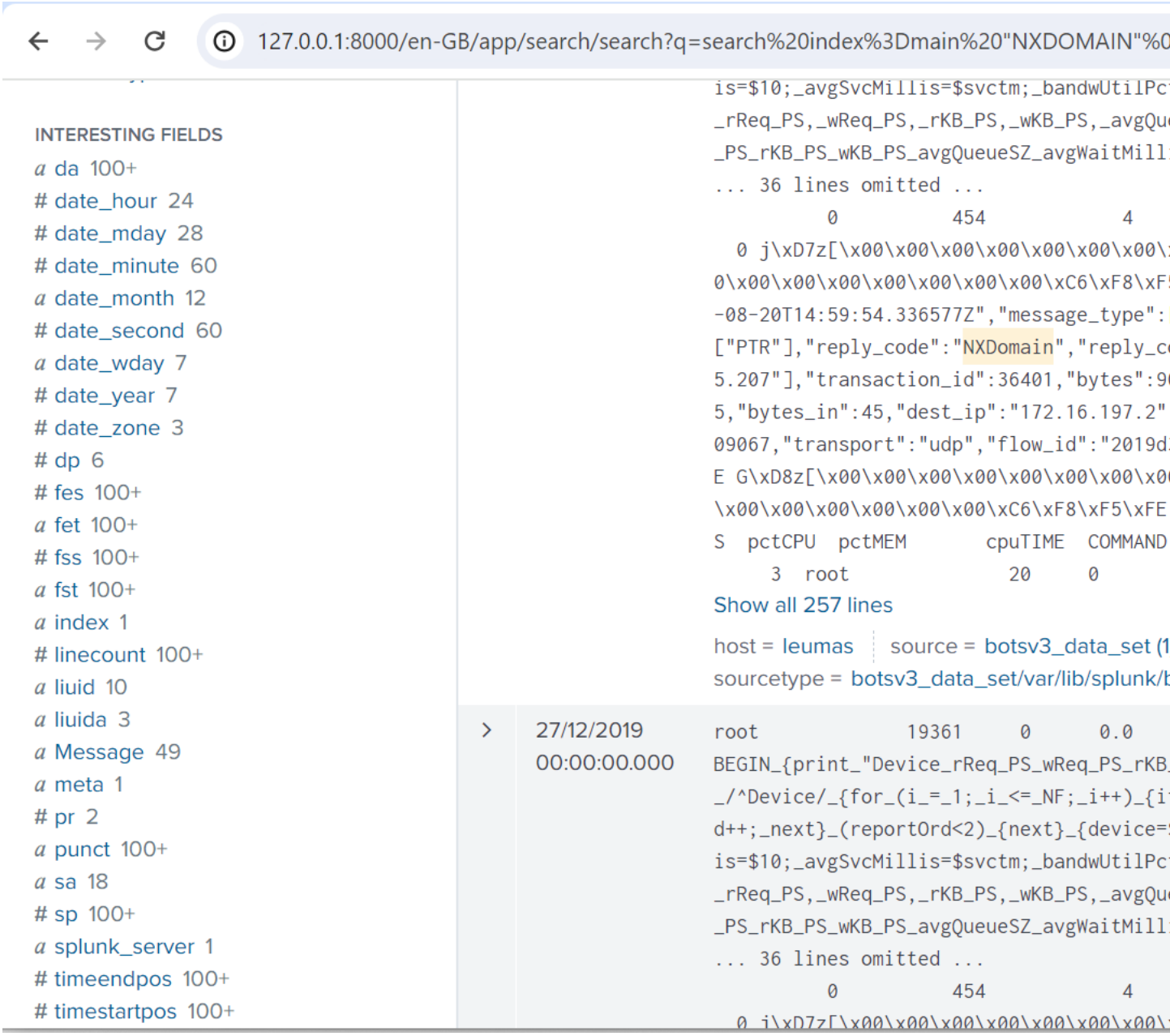
| rex "QUERY\s+(?<domain>\S+)"

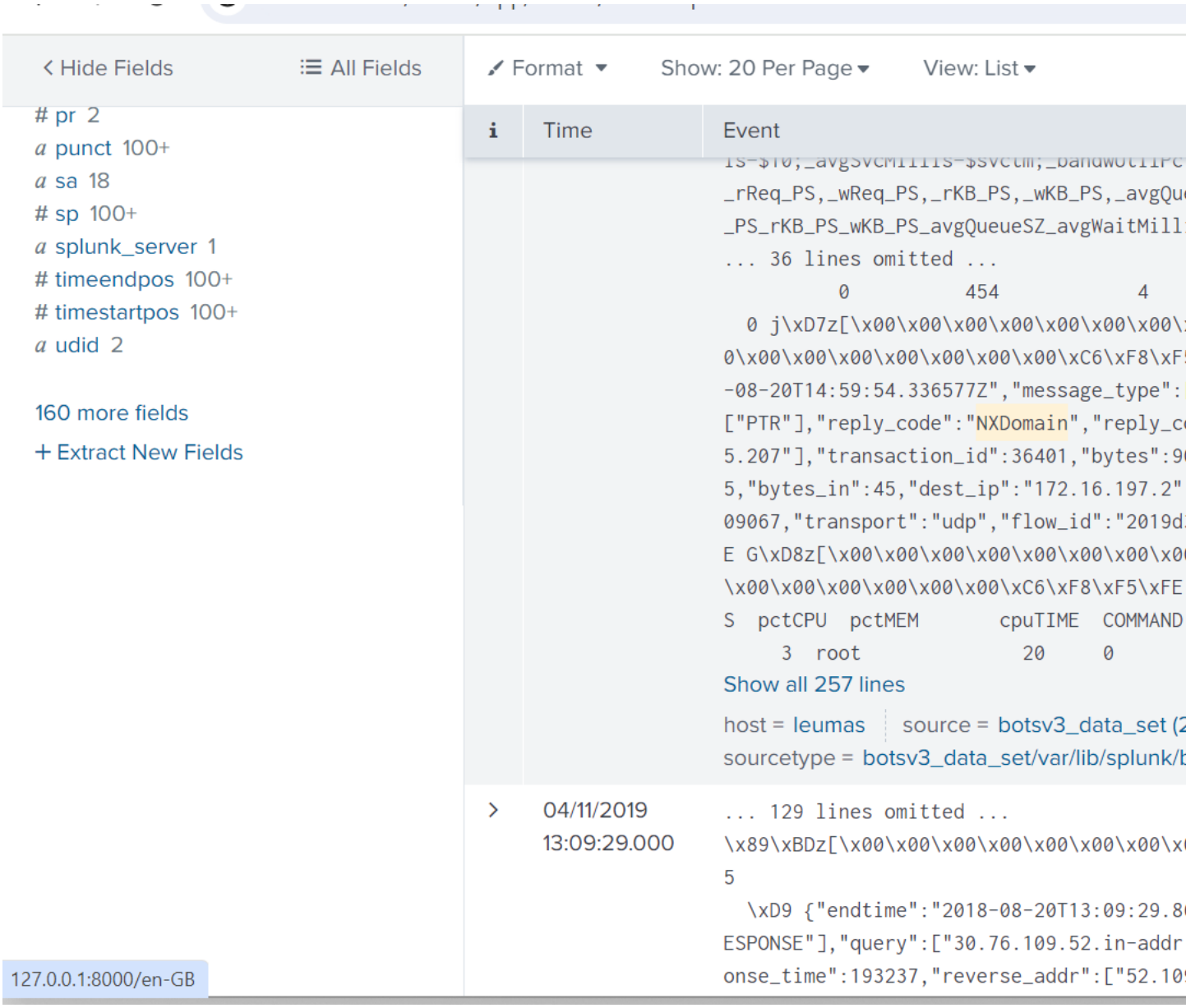
| stats count AS queries BY domain

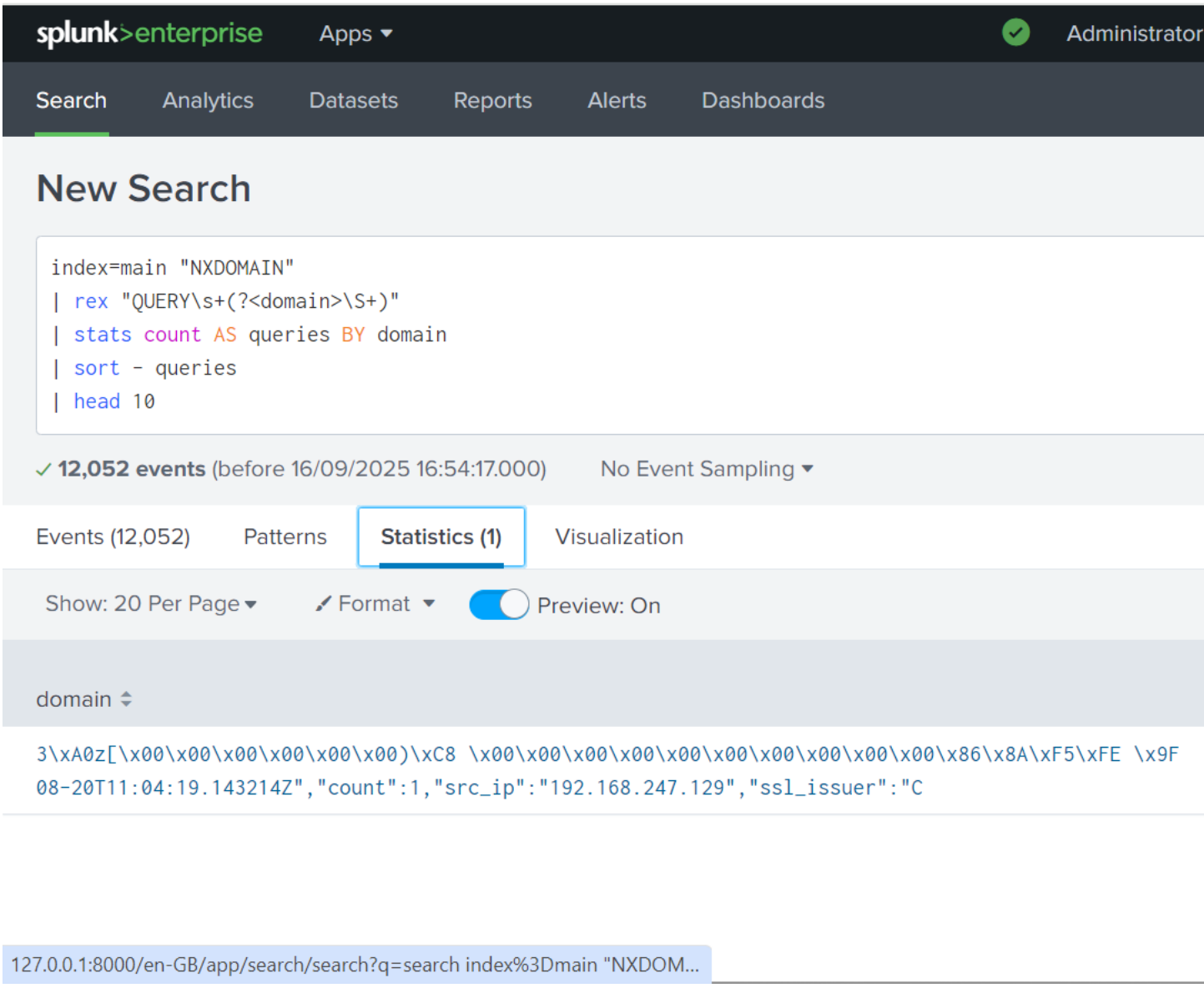
| sort - queries

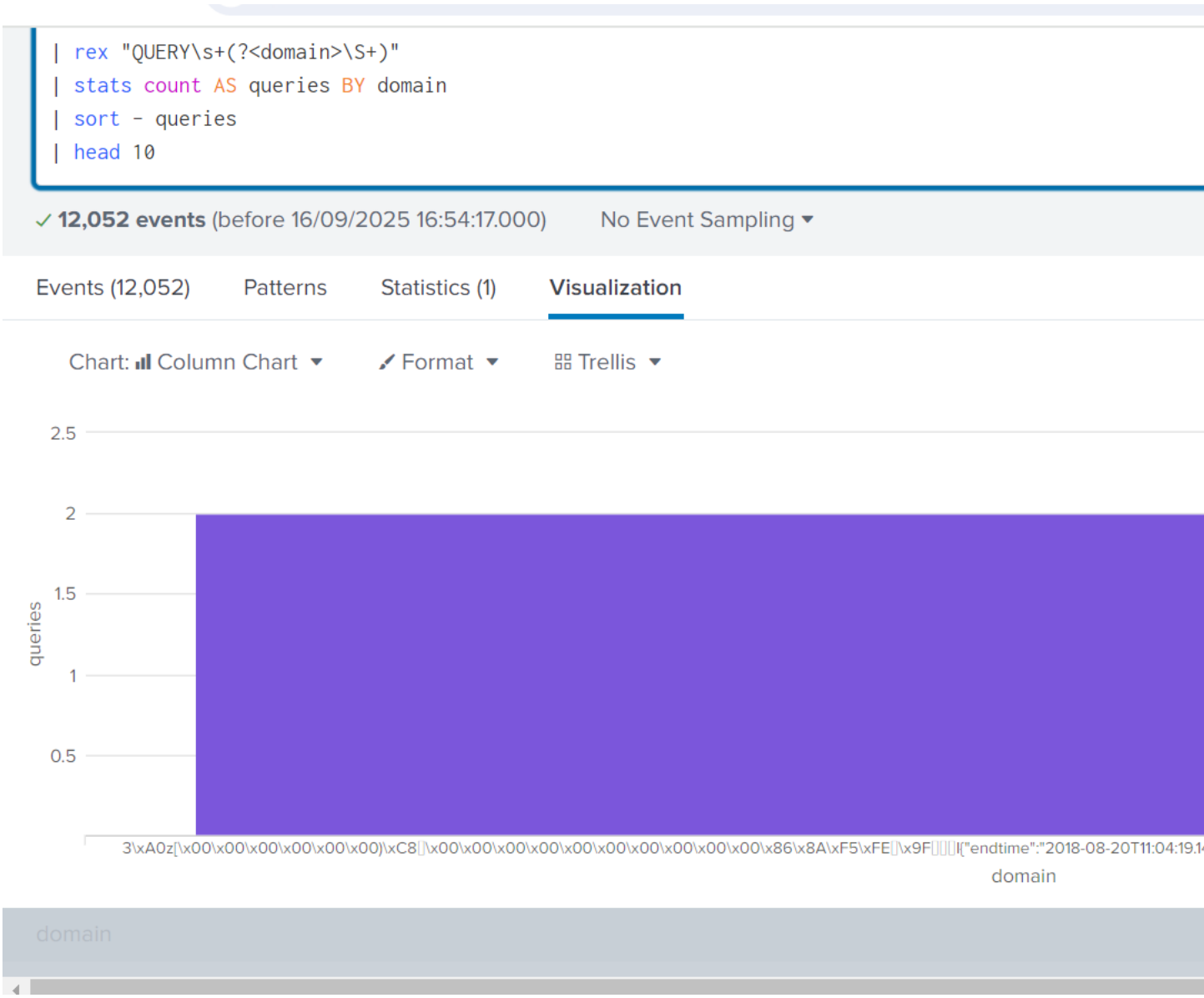
| head 10What It Does


splunk>enterprise
Apps
Administrator
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
index=main "NXDOMAIN"
| rex "QUERY\s+(?<domain>\S+)"
| stats count AS queries BY domain
| sort - queries
| head 10
12,052 events (before 16/09/2025 16:54:17.000)
No Event Sampling
Events (12,052)
Patterns
Statistics (1)
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
Time
Event
27/12/2019
00:00:00.000
root 19361 0 0.0
BEGIN_{print_"Device_rReq_PS_wReq_PS_rKB
127.0.0.1:8000/en-GB/app/search/search?q=search index%3Dmain "NXDOMAIN"%0A%7C rex "QUERY%5Cs%2B(%3F<domain>%5CS%


127.0.0.1:8000/en-GB/app/search/search?q=search%20index%3Dmain%20"NXDOMAIN"%0
INTERESTING FIELDS
a da 100+
date_hour 24
date_mday 28
date_minute 60
a date_month 12
date_second 60
a date_wday 7
date_year 7
date_zone 3
dp 6
fes 100+
a fet 100+
fss 100+
a fst 100+
a index 1
linecount 100+
a liuid 10
a liuida 3
a Message 49
a meta 1
pr 2
a punct 100+
a sa 18
sp 100+
a splunk_server 1
# timeendpos 100+
# timestartpos 100+
is=$10;_avgSvcMillis=$svctm;_bandwUtilPc
_rReq_PS,_wReq_PS,_rKB_PS,_wKB_PS,_avgQu
_PS_rKB_PS_wKB_PS_avgQueueSZ_avgWaitMill
... 36 lines omitted ...
0 454 4
0 j\xD7z[\x00\x00\x00\x00\x00\x00\x00\
0\x00\x00\x00\x00\x00\x00\x00\xC6\xF8\xF
-08-20T14:59:54.336577Z","message_type":
["PTR"],"reply_code":"NXDomain","reply_c
5.207"],"transaction_id":36401,"bytes":9
5,"bytes_in":45,"dest_ip":"172.16.197.2"
09067,"transport":"udp","flow_id":"2019d
E G\xD8z[\x00\x00\x00\x00\x00\x00\x00\x0
\x00\x00\x00\x00\x00\x00\xC6\xF8\xF5\xFE
S pctCPU pctMEM cpuTIME COMMAND
3 root 20 0
Show all 257 lines
host = leumas source = botsv3_data_set (1
sourcetype = botsv3_data_set/var/lib/splunk/b
27/12/2019 00:00:00.000
root 19361 0 0.0
BEGIN_{print_"Device_rReq_PS_wReq_PS_rKB
_/^Device/_{for_(i_=_1;_i_<=_NF;_i++)_{i
d++;_next}_(reportOrd<2)_{next}_{device=
is=$10;_avgSvcMillis=$svctm;_bandwUtilPc
_rReq_PS,_wReq_PS,_rKB_PS,_wKB_PS,_avgQu
_PS_rKB_PS_wKB_PS_avgQueueSZ_avgWaitMill
... 36 lines omitted ...
0 454 4
0 j\xD7z[\x00\x00\x00\x00\x00\x00\x00\


Hide Fields
All Fields
Format
Show: 20 Per Page
View: List
pr 2
a punct 100+
a sa 18
sp 100+
a splunk_server 1
timeendpos 100+
timestartpos 100+
a udid 2
160 more fields
+ Extract New Fields
Time
Event
_rReq_PS,_wReq_PS,_rKB_PS,_wKB_PS,_avgQu
_PS_rKB_PS_wKB_PS_avgQueueSZ_avgWaitMill
... 36 lines omitted ...
0 454 4
0 j\xD7z[\x00\x00\x00\x00\x00\x00\x00\
0\x00\x00\x00\x00\x00\x00\xC6\xF8\xF
-08-20T14:59:54.336577Z","message_type":
["PTR"],"reply_code":"NXDomain","reply_c
5.207"],"transaction_id":36401,"bytes":9
5,"bytes_in":45,"dest_ip":"172.16.197.2"
09067,"transport":"udp","flow_id":"2019d
E G\xD8z[\x00\x00\x00\x00\x00\x00\x00\x0
\x00\x00\x00\x00\x00\x00\xC6\xF8\xF5\xFE
S pctCPU pctMEM cpuTIME COMMAND
3 root 20 0
Show all 257 lines
host = leumas source = botsv3_data_set (2
sourcetype = botsv3_data_set/var/lib/splunk/b
04/11/2019
13:09:29.000
... 129 lines omitted ...
\x89\xBDz[\x00\x00\x00\x00\x00\x00\x00\x
5
\xD9 {"endtime":"2018-08-20T13:09:29.8
ESPONSE"],"query":["30.76.109.52.in-addr
onse_time":193237,"reverse_addr":["52.10
127.0.0.1:8000/en-GB


splunk>enterprise
Apps
Administrator
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
index=main "NXDOMAIN"
| rex "QUERY\s+(?<domain>\S+)"
| stats count AS queries BY domain
| sort - queries
| head 10
12,052 events (before 16/09/2025 16:54:17.000)
No Event Sampling
Events (12,052)
Patterns
Statistics (1)
Visualization
Show: 20 Per Page
Format
Preview: On
domain
3\xA0z[\x00\x00\x00\x00\x00\x00)\xC8 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x86\x8A\xF5\xFE \x9F
08-20T11:04:19.143214Z","count":1,"src_ip":"192.168.247.129","ssl_issuer":"C
127.0.0.1:8000/en-GB/app/search/search?q=search index%3Dmain "NXDOM...



- Extracts the queried **domain** from raw events using rex.
- Counts how many times each domain caused an NXDOMAIN response.
- Returns the **top 10 most queried domains**.

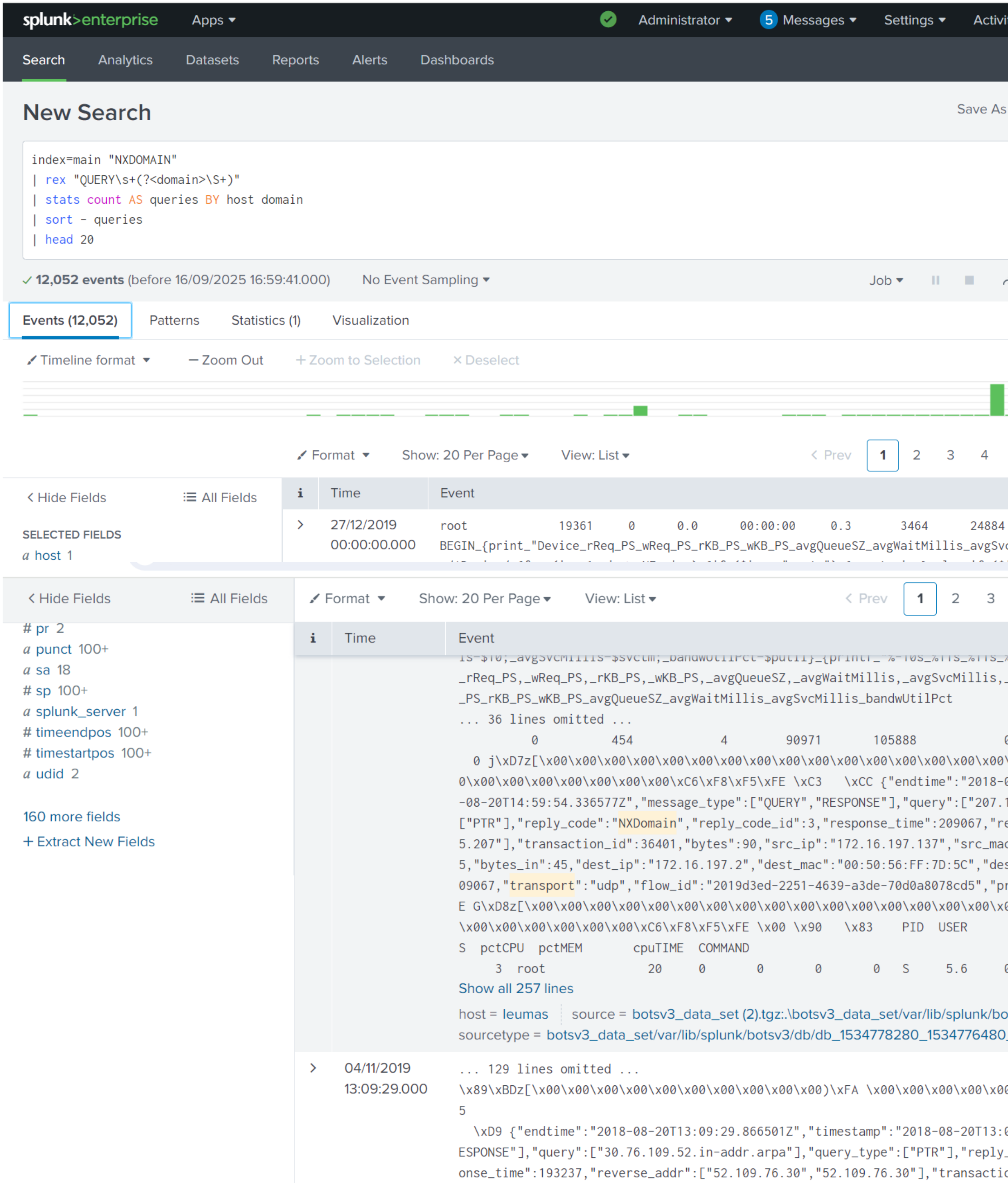
When to Use

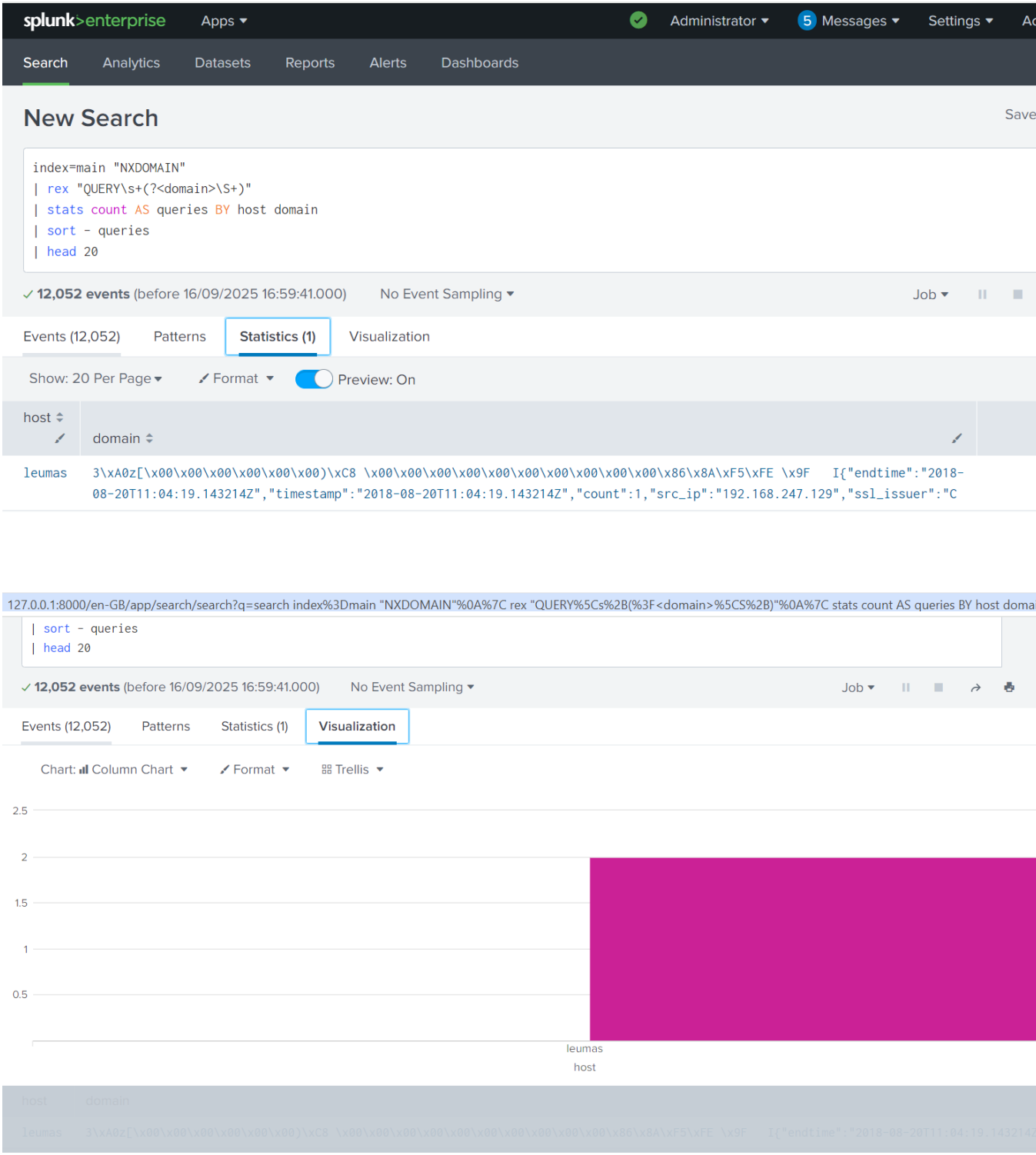
- To detect **frequently misconfigured domains**.
- To spot potential **malicious DNS tunneling** or **C2 traffic**.

Top Queried Domains Per Host

Query

```
index=main "NXDOMAIN"
| rex "QUERY\s+(?<domain>\S+)"
| stats count AS queries BY host domain
| sort - queries
| head 20
```


splunk>enterprise
Apps
Administrator
5 Messages
Settings
Activity
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
Save As
index=main "NXDOMAIN"
| rex "QUERY\s+(?<domain>\S+)"
| stats count AS queries BY host domain
| sort - queries
| head 20
✓ 12,052 events (before 16/09/2025 16:59:41.000)
No Event Sampling
Job
Events (12,052)
Patterns
Statistics (1)
Visualization
Timeline format
— Zoom Out
+ Zoom to Selection
× Deselect
Format
Show: 20 Per Page
View: List
Prev
1 2 3 4
Hide Fields
All Fields
SELECTED FIELDS
a host 1
i
Time
Event
27/12/2019 00:00:00.000
root 19361 0 0.0 00:00:00 0.3 3464 24884
BEGIN_{print_"Device_rReq_PS_wReq_PS_rKB_PS_wKB_PS_avgQueueSZ_avgWaitMillis_avgSvcM
Hide Fields
All Fields
Format
Show: 20 Per Page
View: List
Prev
1 2 3
pr 2
a punct 100+
a sa 18
sp 100+
a splunk_server 1
timeendpos 100+
timestartpos 100+
a udid 2
160 more fields
+ Extract New Fields
i
Time
Event
_rReq_PS,_wReq_PS,_rKB_PS,_wKB_PS,_avgQueueSZ,_avgWaitMillis,_avgSvcMillis,_b
_PS_rKB_PS_wKB_PS_avgQueueSZ_avgWaitMillis_avgSvcMillis_bandwUtilPct
... 36 lines omitted ...
0 454 4 90971 105888 0
0 j\xD7z[\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
0\x00\x00\x00\x00\x00\x00\x00\xC6\xF8\xF5\xFE \xC3 \xCC {"endtime":"2018-08
-08-20T14:59:54.336577Z","message_type":["QUERY","RESPONSE"],"query":["207.16
["PTR"],"reply_code":"NXDomain","reply_code_id":3,"response_time":209067,"rev
5.207"],"transaction_id":36401,"bytes":90,"src_ip":"172.16.197.137","src_mac"
5,"bytes_in":45,"dest_ip":"172.16.197.2","dest_mac":"00:50:56:FF:7D:5C","dest
09067,"transport":"udp","flow_id":"2019d3ed-2251-4639-a3de-70d0a8078cd5","pro
E G\xD8z[\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\xC6\xF8\xF5\xFE \x00 \x90 \x83 PID USER
S pctCPU pctMEM cpuTIME COMMAND
3 root 20 0 0 0 0 S 5.6 0.
Show all 257 lines
host = leumas
source = botsv3_data_set (2).tgz:.\botsv3_data_set/var/lib/splunk/bots
sourcetype = botsv3_data_set/var/lib/splunk/botsv3/db/db_1534778280_1534776480_
04/11/2019 13:09:29.000
... 129 lines omitted ...
\x89\xBDz[\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00)\xFA \x00\x00\x00\x00\x00\
5
\xD9 {"endtime":"2018-08-20T13:09:29.866501Z","timestamp":"2018-08-20T13:09
ESPONSE"],"query":["30.76.109.52.in-addr.arpa"],"query_type":["PTR"],"reply_c
onse_time":193237,"reverse_addr":["52.109.76.30","52.109.76.30"],"transaction



What It Does

- Breaks down top queried domains **per originating host**.
- Useful for pinpointing **which machines** are causing repeated NXDOMAIN lookups.

Top source IPs making DNS requests:

```
index=main "NXDOMAIN"
| stats count AS dns_requests BY src_ip
| sort - dns_requests
| head 10
```

```
index=main "NXDOMAIN"
| stats count AS dns_requests BY src_ip
| sort - dns_requests
| head 10
```

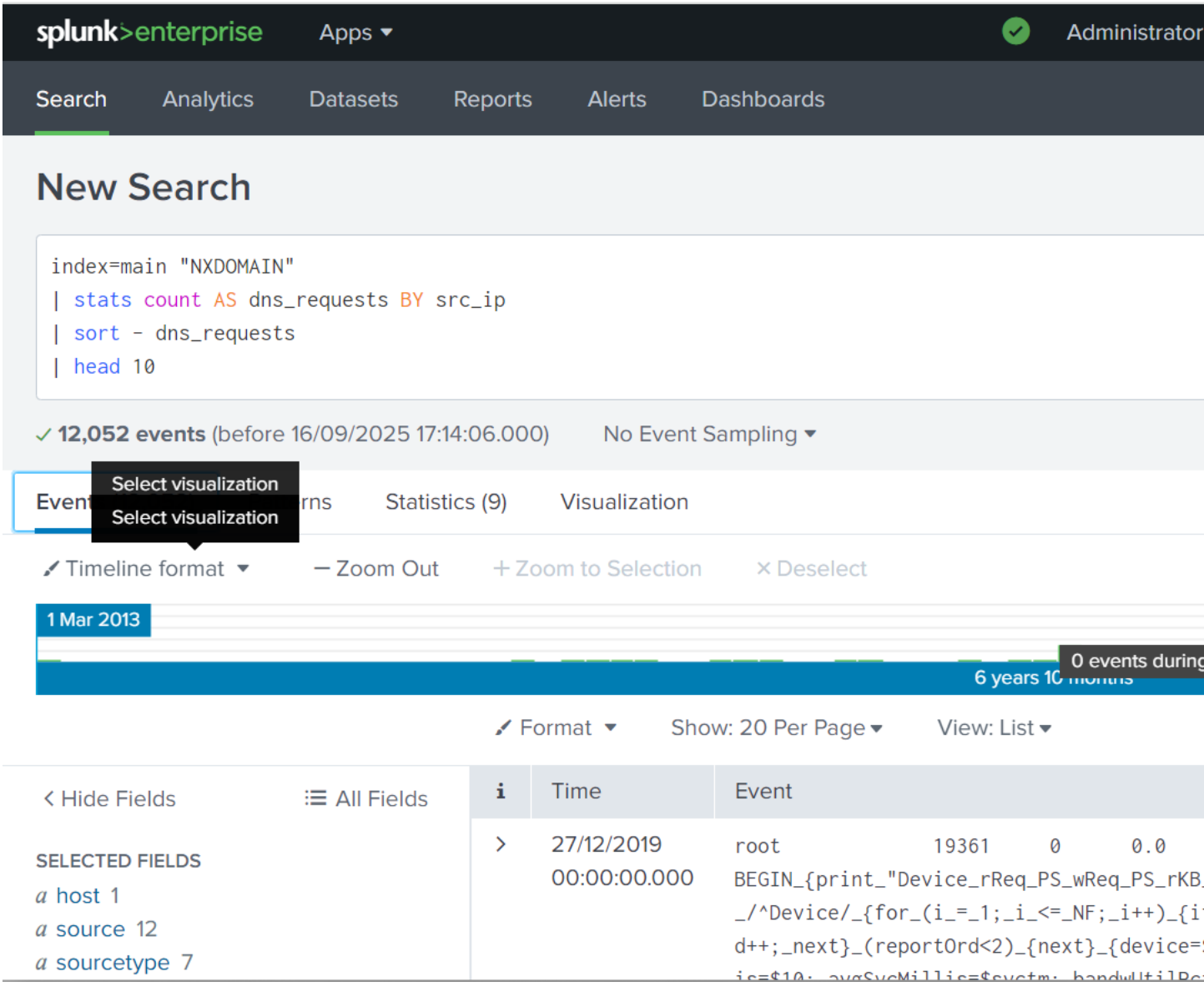
✓ **12,052 events** (before 16/09/2025 17:14:06.000) No Event Sampling

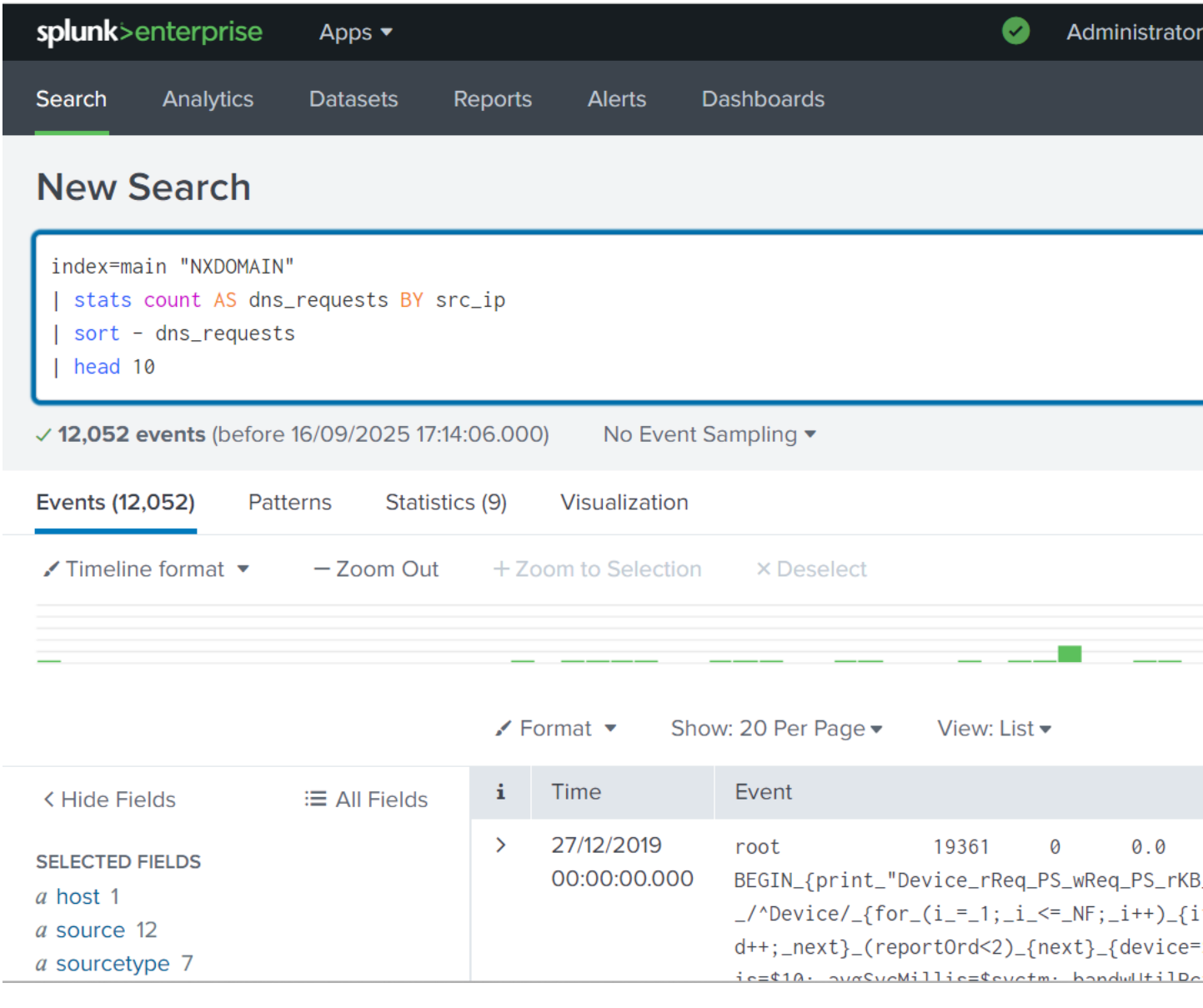
Select visualization
Select visualization

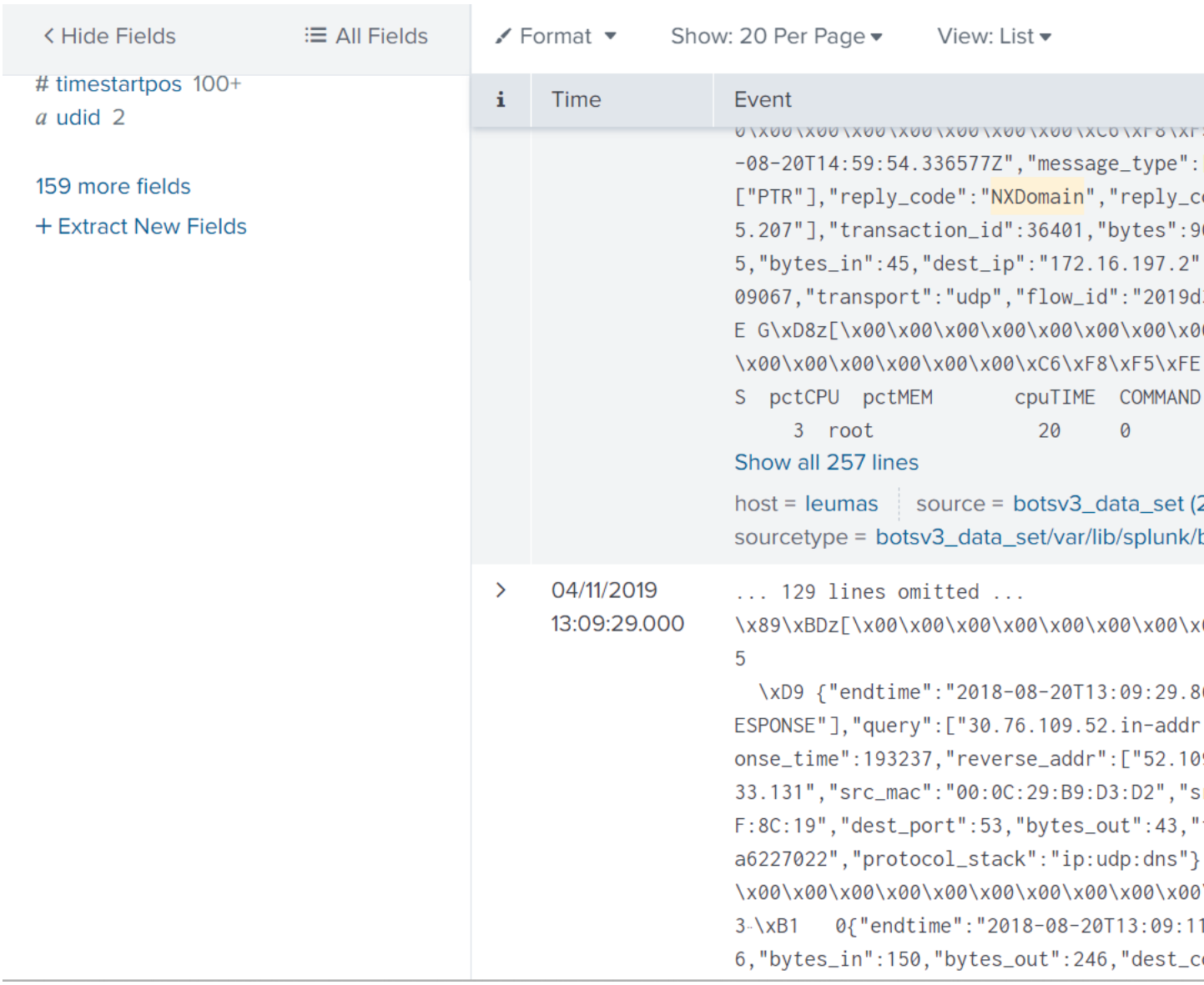
Event ns **Statistics (9)** Visualization

Show: 20 Per Page Format Preview: On

src_ip
192.168.24.128
192.168.247.131
192.168.3.130
172.16.197.137
192.168.70.186
172.16.133.131
192.168.105.215
192.168.247.129
74.125.195.189


splunk>enterprise
Apps
Administrator
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
index=main "NXDOMAIN"
| stats count AS dns_requests BY src_ip
| sort - dns_requests
| head 10
12,052 events (before 16/09/2025 17:14:06.000)
No Event Sampling
Select visualization
Select visualization
Statistics (9)
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 Mar 2013
0 events during
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 12
a sourcetype 7
Time
Event
27/12/2019
00:00:00.000
root 19361 0 0.0
BEGIN_{print_"Device_rReq_PS_wReq_PS_rKB
_/^Device/_{for_(i_=_1;_i_<=_NF;_i++)_{i
d++;_next}_(reportOrd<2)_{next}_{device=


splunk>enterprise
Apps
Administrator
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
index=main "NXDOMAIN"
| stats count AS dns_requests BY src_ip
| sort - dns_requests
| head 10
✓ 12,052 events (before 16/09/2025 17:14:06.000)
No Event Sampling
Events (12,052)
Patterns
Statistics (9)
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 12
a sourcetype 7
Time
Event
27/12/2019
00:00:00.000
root 19361 0 0.0
BEGIN_{print_"Device_rReq_PS_wReq_PS_rKB
_/^Device/_{for_(i_=_1;_i_<=_NF;_i++)_{i
d++;_next}_(reportOrd<2)_{next}_{device=



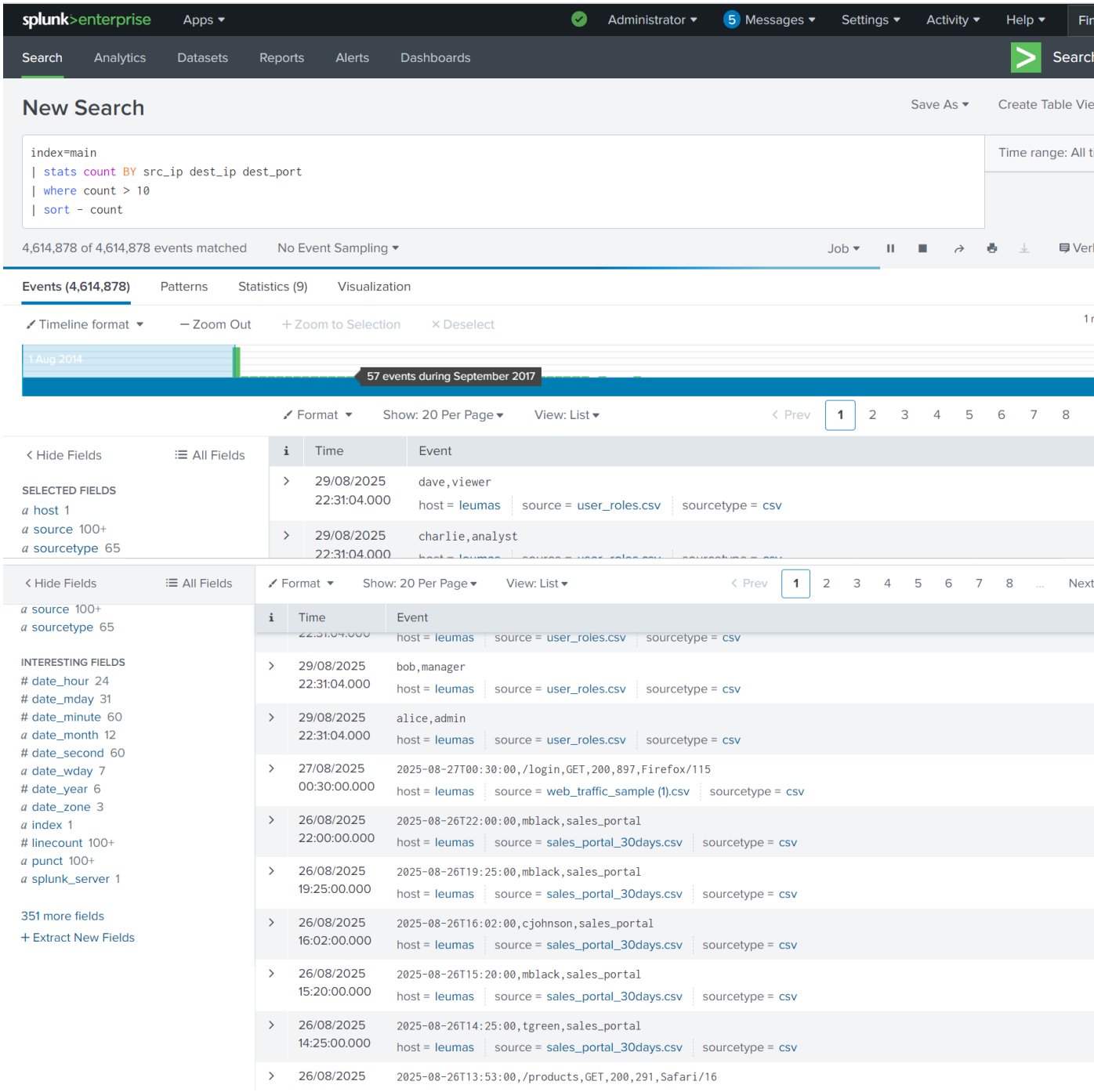
Why This Works

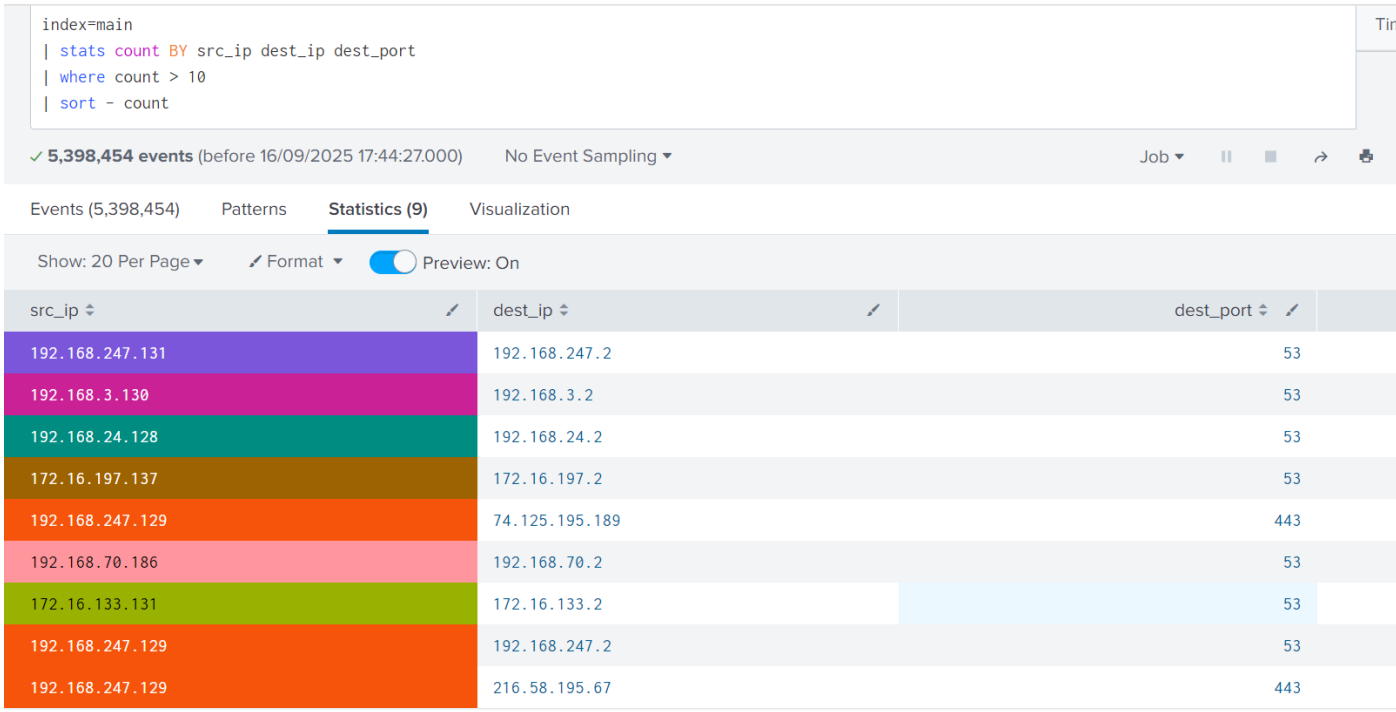
- **index=main "NXDOMAIN"** – Filters only DNS events in the main index that include "NXDOMAIN".
- **stats count AS dns_requests BY src_ip** – Counts the number of such events for each source IP address.
- **sort - dns_requests** – Sorts results by count, descending.
- **head 10** – Returns only the top 10 IPs.

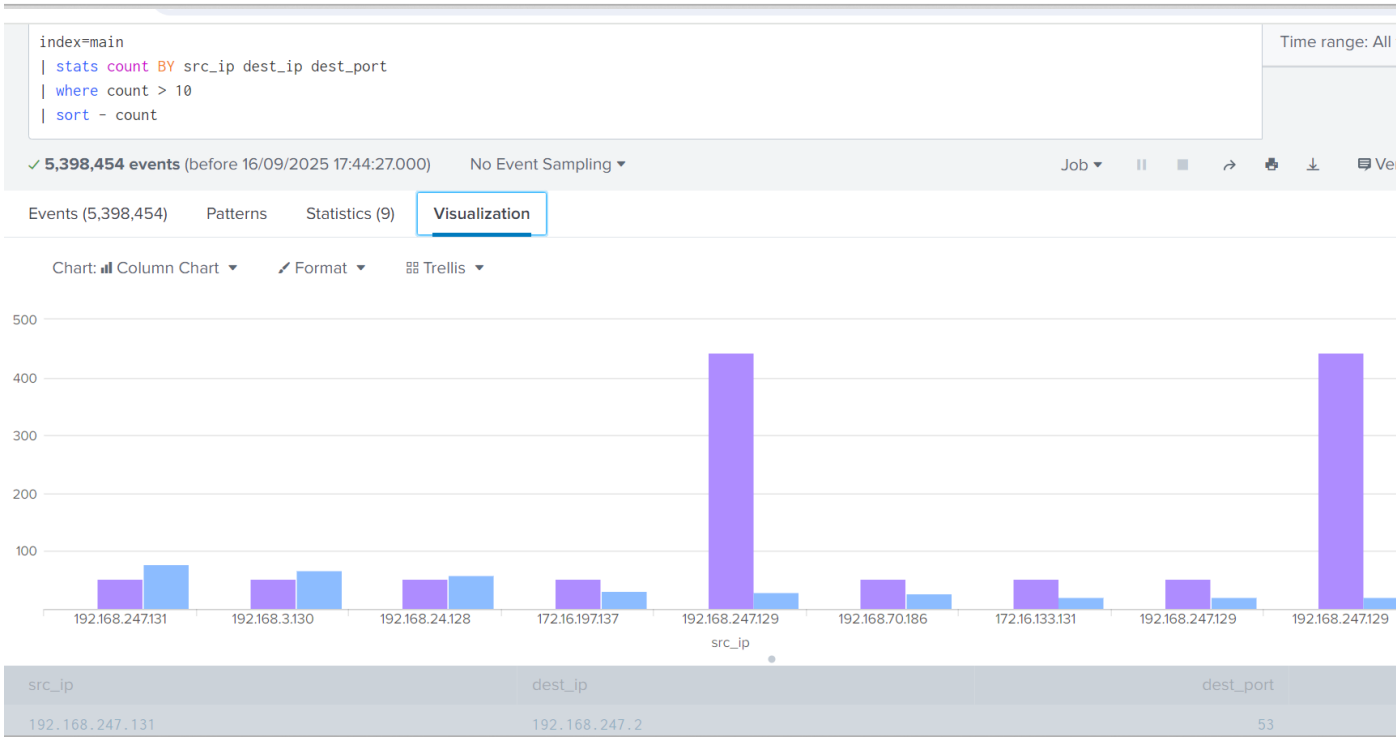
Malware Beaconing Detection

Purpose

Detect potential **command-and-control (C2) beaconing** behavior by identifying repeated outbound connections from the same host to the same destination. High repetition can indicate malware beaconing to a remote server.







? How It Works

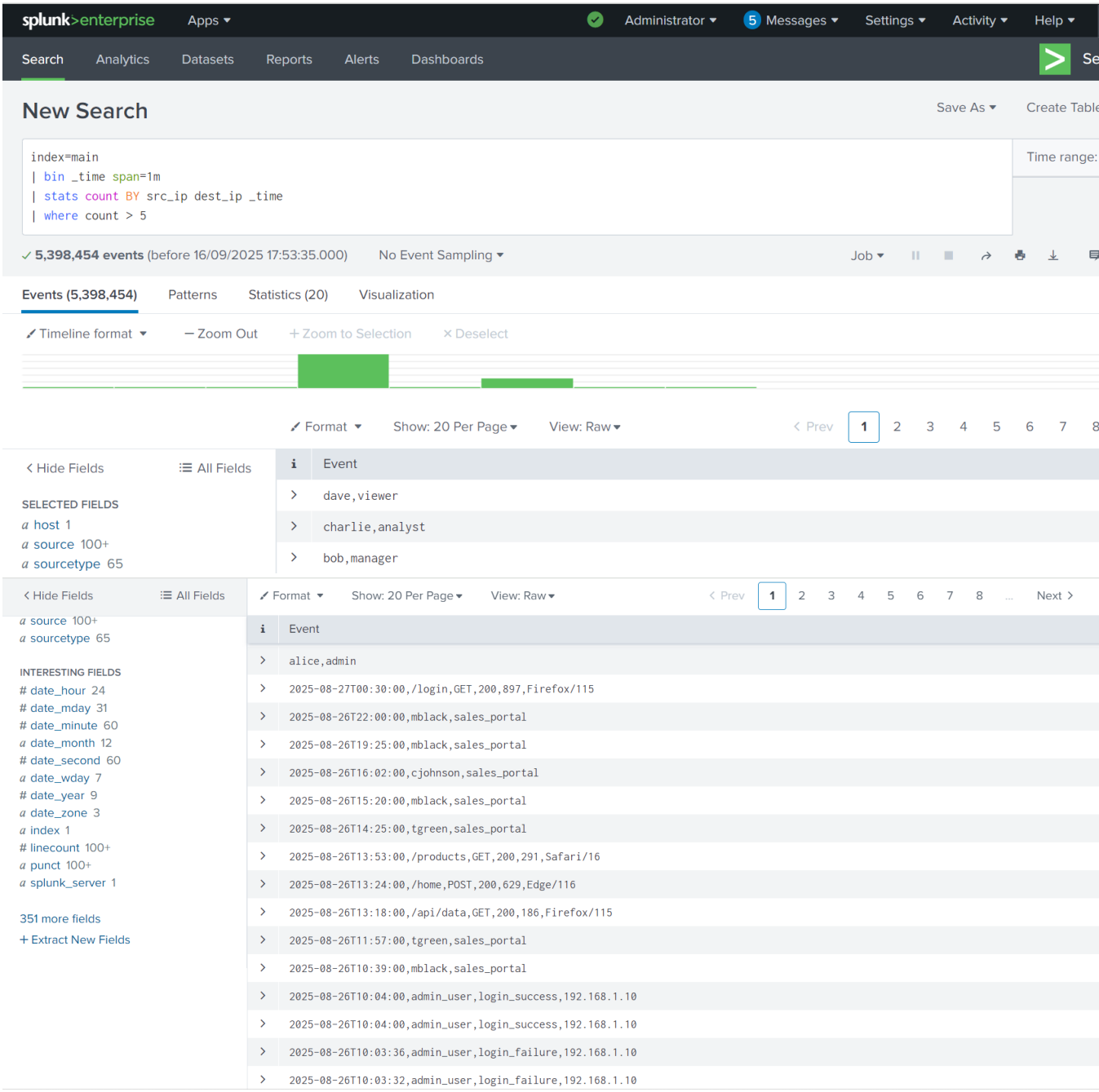
Component	Description

Component	Description
index=main	Searches all events in the main index.
stats count BY src_ip dest_ip dest_port	Groups events by **source IP**, **destination IP**, and **destination port**, counting how many times each combination appears.
where count > 10	Filters for entries with more than **10 occurrences** (adjust based on network traffic volume).
sort - count	Sorts results in descending order so the most frequent combinations appear first

Detect Regular-Interval Connections – Documentation

Objective

Identify hosts making **frequent outbound connections at regular intervals**, which may indicate **malware beaconing** or **automated scanning activity**.


splunk>enterprise
Apps
Administrator
5 Messages
Settings
Activity
Help
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
Save As
Create Table
index=main
| bin _time span=1m
| stats count BY src_ip dest_ip _time
| where count > 5
Time range:
5,398,454 events (before 16/09/2025 17:53:35.000)
No Event Sampling
Job
Events (5,398,454)
Patterns
Statistics (20)
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
Format
Show: 20 Per Page
View: Raw
Prev
1
2
3
4
5
6
7
8
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 100+
a sourcetype 65
Event
dave,viewer
charlie,analyst
bob,manager
Hide Fields
All Fields
Format
Show: 20 Per Page
View: Raw
Prev
1
2
3
4
5
6
7
8
...
Next
a source 100+
a sourcetype 65
INTERESTING FIELDS
date_hour 24
date_mday 31
date_minute 60
a date_month 12
date_second 60
a date_wday 7
date_year 9
a date_zone 3
a index 1
linecount 100+
a punct 100+
a splunk_server 1
351 more fields
+ Extract New Fields
Event
alice,admin
2025-08-27T00:30:00,/login,GET,200,897,Firefox/115
2025-08-26T22:00:00,mblack,sales_portal
2025-08-26T19:25:00,mblack,sales_portal
2025-08-26T16:02:00,cjohnson,sales_portal
2025-08-26T15:20:00,mblack,sales_portal
2025-08-26T14:25:00,tgreen,sales_portal
2025-08-26T13:53:00,/products,GET,200,291,Safari/16
2025-08-26T13:24:00,/home,POST,200,629,Edge/116
2025-08-26T13:18:00,/api/data,GET,200,186,Firefox/115
2025-08-26T11:57:00,tgreen,sales_portal
2025-08-26T10:39:00,mblack,sales_portal
2025-08-26T10:04:00,admin_user,login_success,192.168.1.10
2025-08-26T10:04:00,admin_user,login_success,192.168.1.10
2025-08-26T10:03:36,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:32,admin_user,login_failure,192.168.1.10

```
| where count > 5
```

✓ **5,398,454 events** (before 16/09/2025 17:53:35.000) No Event Sampling Job

Events (5,398,454) Patterns **Statistics (20)** Visualization

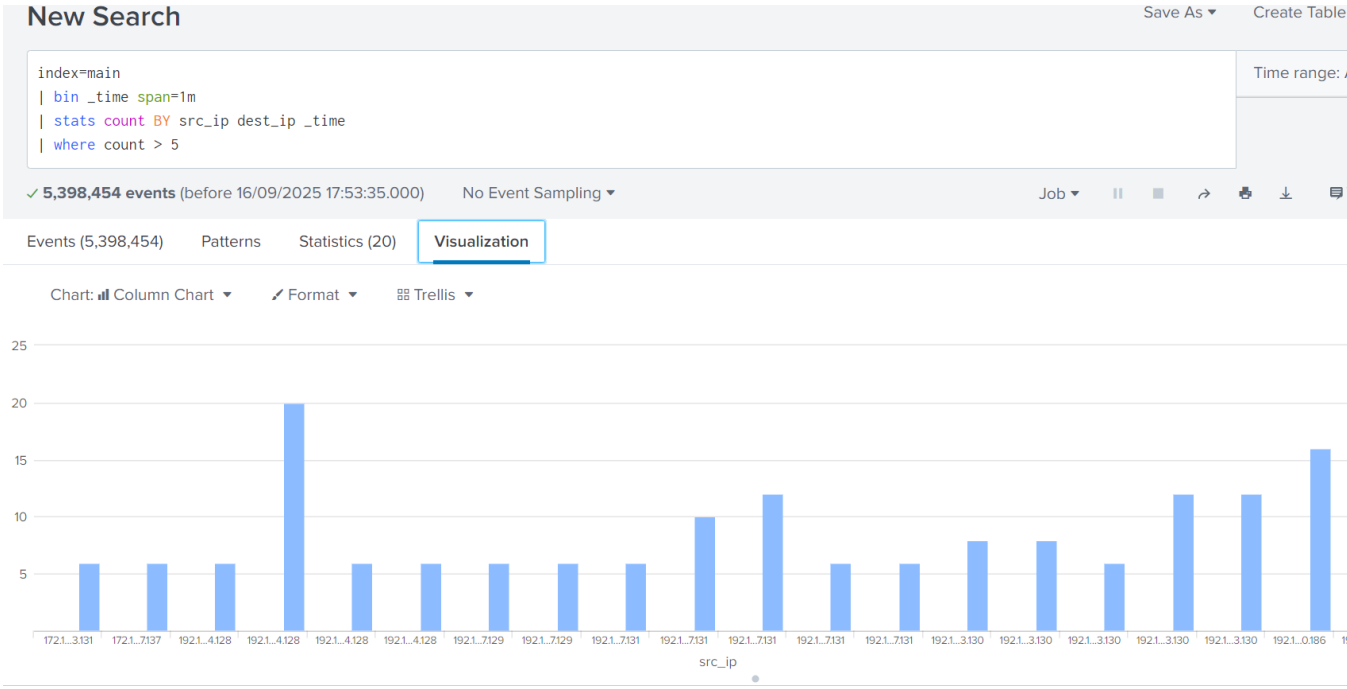
Show: 20 Per Page Format Preview: On

src_ip	dest_ip	_time
172.16.133.131	172.16.133.2	2018-08-20 14:25:00
172.16.197.137	172.16.197.2	2018-08-20 16:13:00
192.168.24.128	192.168.24.2	2018-08-20 12:27:00
192.168.24.128	192.168.24.2	2018-08-20 12:32:00
192.168.24.128	192.168.24.2	2018-08-20 12:33:00
192.168.24.128	216.58.192.2	2018-08-20 12:32:00
192.168.247.129	216.58.195.67	2018-08-20 12:18:00
192.168.247.129	216.58.195.67	2018-08-20 12:19:00
192.168.247.131	192.168.247.2	2018-08-20 12:17:00
192.168.247.131	192.168.247.2	2018-08-20 12:19:00
192.168.247.131	192.168.247.2	2018-08-20 12:30:00
192.168.247.131	192.168.247.2	2018-08-20 14:54:00

127.0.0.1:8000/en-GB/app/search/search?q=search%20index%3Dmain%0A%7C%20bin%20_time%20span%3D1m%0A%7C%20stats%20count%20BY%20src_ip%...

Show: 20 Per Page Format Preview: On

src_ip	dest_ip	_time	co
192.168.24.128	216.58.192.2	2018-08-20 12:32:00	
192.168.247.129	216.58.195.67	2018-08-20 12:18:00	
192.168.247.129	216.58.195.67	2018-08-20 12:19:00	
192.168.247.131	192.168.247.2	2018-08-20 12:17:00	
192.168.247.131	192.168.247.2	2018-08-20 12:19:00	
192.168.247.131	192.168.247.2	2018-08-20 12:30:00	
192.168.247.131	192.168.247.2	2018-08-20 14:54:00	
192.168.247.131	192.168.247.2	2018-08-20 20:03:00	
192.168.3.130	192.168.3.2	2018-08-20 12:20:00	
192.168.3.130	192.168.3.2	2018-08-20 12:21:00	
192.168.3.130	192.168.3.2	2018-08-20 12:22:00	
192.168.3.130	192.168.3.2	2018-08-20 12:35:00	
192.168.3.130	192.168.3.2	2018-08-20 12:36:00	
192.168.70.186	192.168.70.2	2018-08-20 12:17:00	
192.168.70.186	192.168.70.2	2018-08-20 12:21:00	



Identify hosts (src_ip) making repeated outbound connections to the same destination (dest_ip) within a short, regular interval (1 minute). This pattern may indicate command-and-control (C2) beaconing by malware.

Steps:

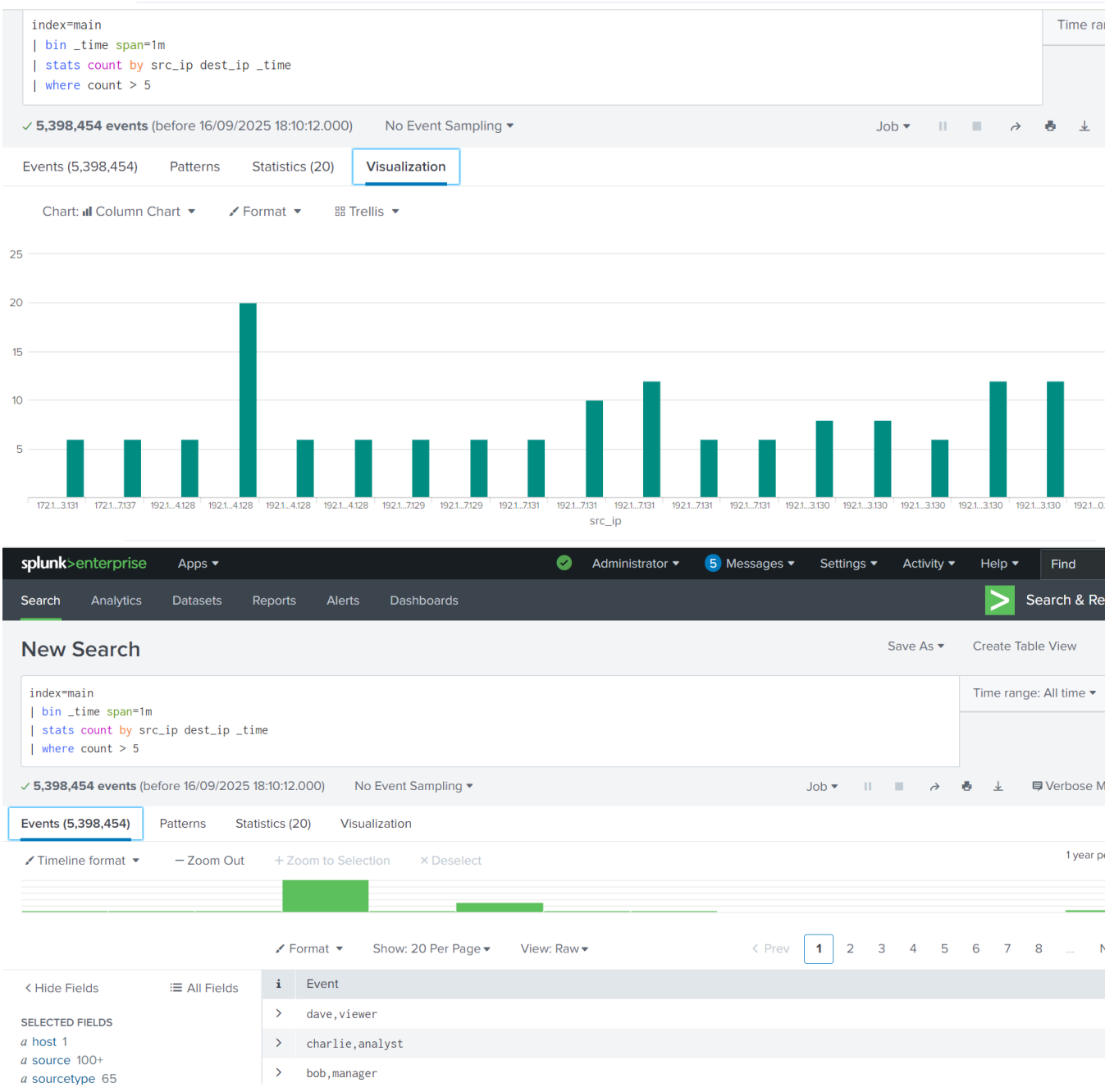
1. **index=main**
   - Searches all logs stored in the main index.
2. **bin _time span=1m**
   - Buckets the event timestamps into **1-minute intervals** to group connections by minute.
3. **stats count by src_ip dest_ip _time**
   - Aggregates the number of connections (count) per **source IP**, **destination IP**, and **time bucket**.
4. **where count > 5**
   - Filters results to show only combinations where more than **5 connections** occurred within a single minute.
   - Threshold 5 can be adjusted depending on network baseline traffic.

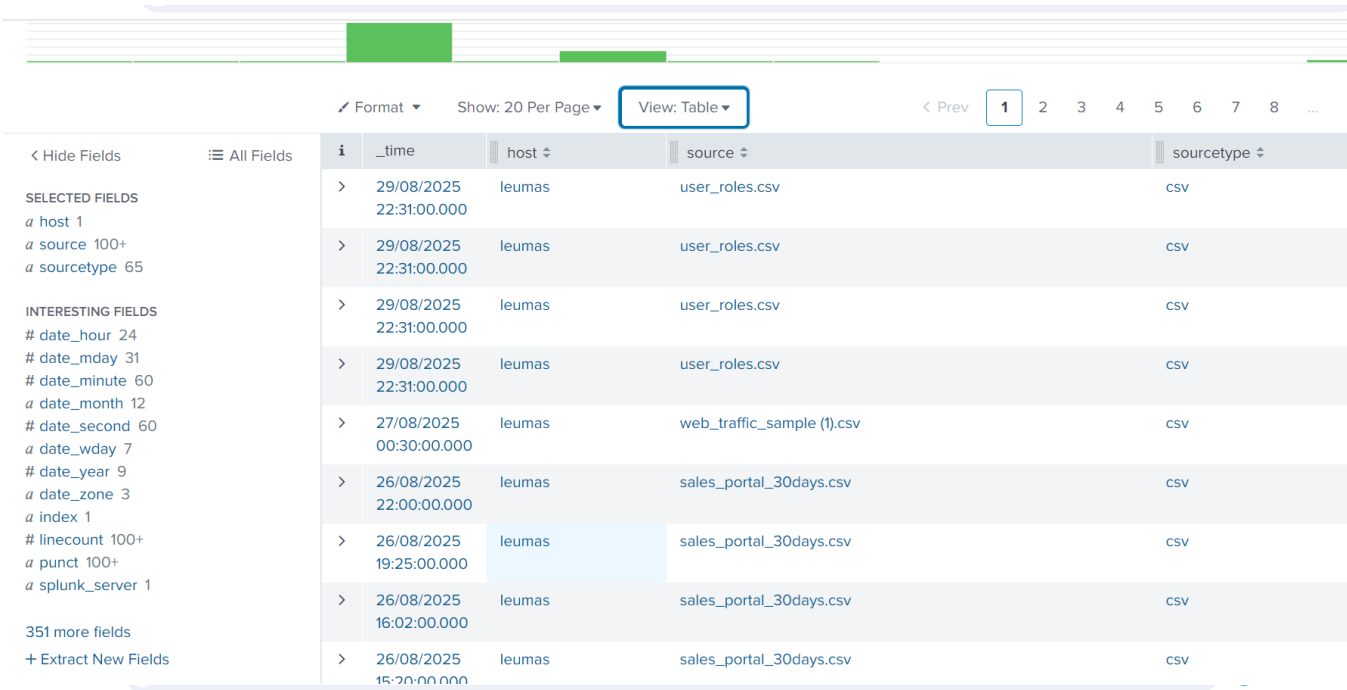
Detect regular-interval connections (aggregate per minute):

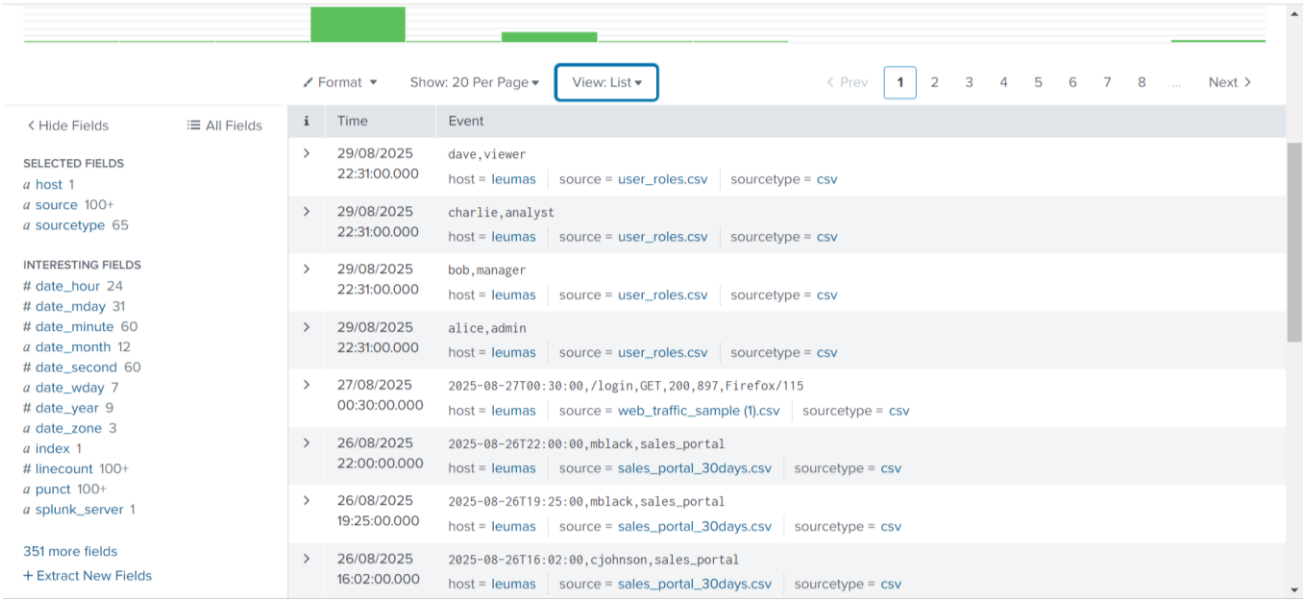
Query

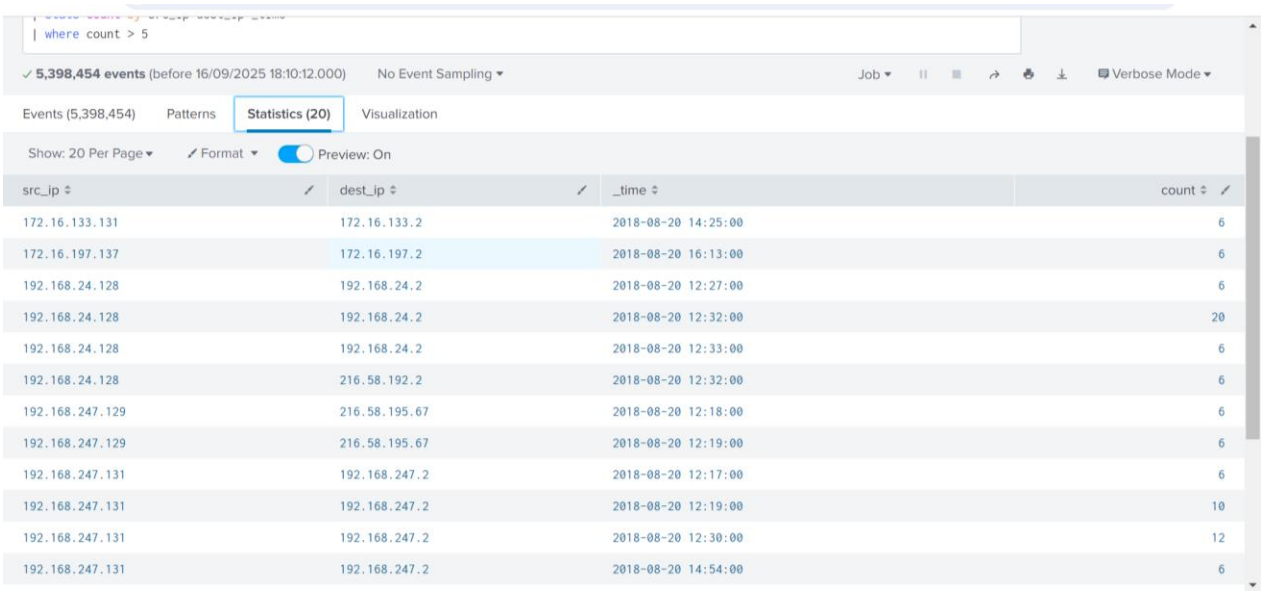
```
index=main
| bin _time span=1m
| stats count by src_ip dest_ip _time
```

| where count > 5




Format
Show: 20 Per Page
View: Table
Prev
1
2
3
4
5
6
7
8
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 100+
a sourcetype 65
INTERESTING FIELDS
date_hour 24
date_mday 31
date_minute 60
a date_month 12
date_second 60
a date_wday 7
date_year 9
a date_zone 3
a index 1
linecount 100+
a punct 100+
a splunk_server 1
351 more fields
+ Extract New Fields
_time
host
source
sourcetype
29/08/2025 22:31:00.000 leumas user_roles.csv csv
29/08/2025 22:31:00.000 leumas user_roles.csv csv
29/08/2025 22:31:00.000 leumas user_roles.csv csv
29/08/2025 22:31:00.000 leumas user_roles.csv csv
27/08/2025 00:30:00.000 leumas web_traffic_sample (1).csv csv
26/08/2025 22:00:00.000 leumas sales_portal_30days.csv csv
26/08/2025 19:25:00.000 leumas sales_portal_30days.csv csv
26/08/2025 16:02:00.000 leumas sales_portal_30days.csv csv
26/08/2025 15:20:00.000 leumas sales_portal_30days.csv csv


Format
Show: 20 Per Page
View: List
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 100+
a sourcetype 65
INTERESTING FIELDS
date_hour 24
date_mday 31
date_minute 60
a date_month 12
date_second 60
a date_wday 7
date_year 9
a date_zone 3
a index 1
linecount 100+
a punct 100+
a splunk_server 1
351 more fields
+ Extract New Fields
Time
Event
29/08/2025 22:31:00.000 dave,viewer host = leumas source = user_roles.csv sourcetype = csv
29/08/2025 22:31:00.000 charlie,analyst host = leumas source = user_roles.csv sourcetype = csv
29/08/2025 22:31:00.000 bob,manager host = leumas source = user_roles.csv sourcetype = csv
29/08/2025 22:31:00.000 alice,admin host = leumas source = user_roles.csv sourcetype = csv
27/08/2025 00:30:00.000 2025-08-27T00:30:00,/login,GET,200,897,Firefox/115 host = leumas source = web_traffic_sample (1).csv sourcetype = csv
26/08/2025 22:00:00.000 2025-08-26T22:00:00,mblack,sales_portal host = leumas source = sales_portal_30days.csv sourcetype = csv
26/08/2025 19:25:00.000 2025-08-26T19:25:00,mblack,sales_portal host = leumas source = sales_portal_30days.csv sourcetype = csv
26/08/2025 16:02:00.000 2025-08-26T16:02:00,cjohnson,sales_portal host = leumas source = sales_portal_30days.csv sourcetype = csv



src_ip	dest_ip	_time	count
172.16.133.131	172.16.133.2	2018-08-20 14:25:00	6
172.16.197.137	172.16.197.2	2018-08-20 16:13:00	6
192.168.24.128	192.168.24.2	2018-08-20 12:27:00	6
192.168.24.128	192.168.24.2	2018-08-20 12:32:00	20
192.168.24.128	192.168.24.2	2018-08-20 12:33:00	6
192.168.24.128	216.58.192.2	2018-08-20 12:32:00	6
192.168.247.129	216.58.195.67	2018-08-20 12:18:00	6
192.168.247.129	216.58.195.67	2018-08-20 12:19:00	6
192.168.247.131	192.168.247.2	2018-08-20 12:17:00	6
192.168.247.131	192.168.247.2	2018-08-20 12:19:00	10
192.168.247.131	192.168.247.2	2018-08-20 12:30:00	12
192.168.247.131	192.168.247.2	2018-08-20 14:54:00	6

Objective:
Identify hosts (src_ip) making repeated outbound connections to the same destination (dest_ip) within a short, regular interval (1 minute). This pattern may indicate command-and-control (C2) beaconing by malware.

Steps:

1. **index=main**
   - Searches all logs stored in the main index.
2. **bin _time span=1m**
   - Buckets the event timestamps into **1-minute intervals** to group connections by minute.
3. **stats count by src_ip dest_ip _time**
   - Aggregates the number of connections (count) per **source IP**, **destination IP**, and **time bucket**.
4. **where count > 5**
   - Filters results to show only combinations where more than **5 connections** occurred within a single minute.
   - Threshold 5 can be adjusted depending on network baseline traffic

   4) Brute-Force Login Detection

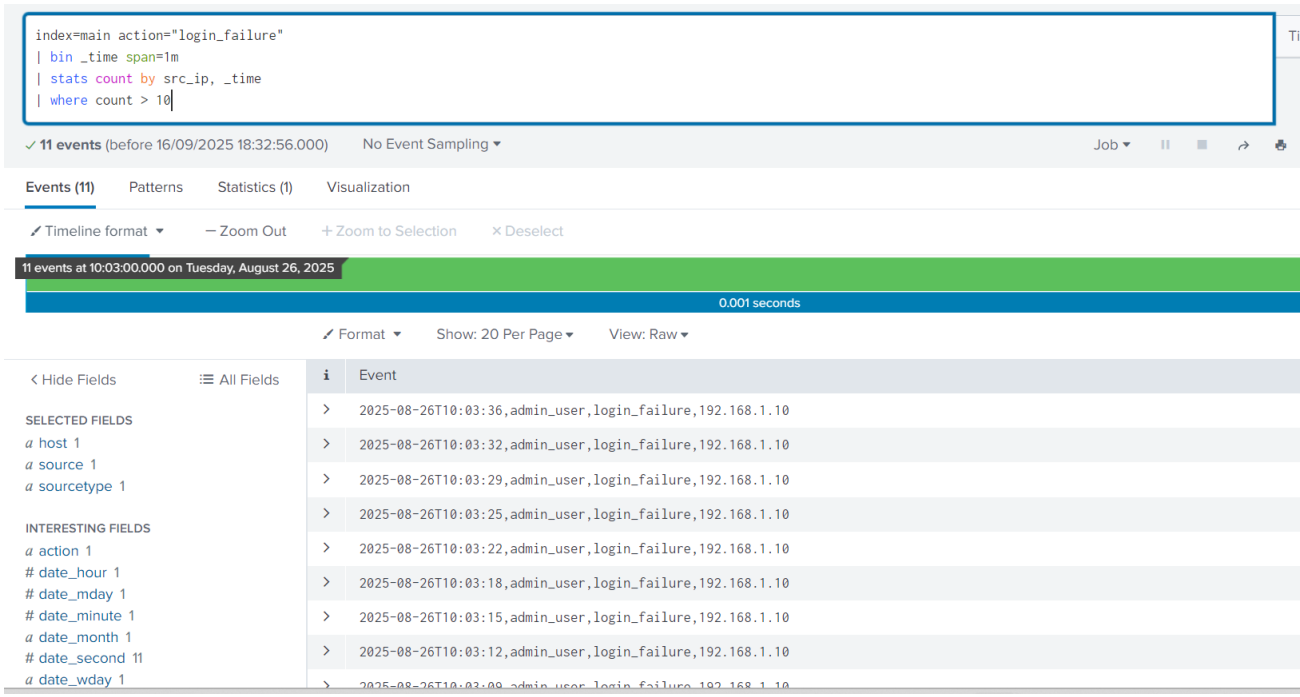
   Detect >10 failed logins per IP within 1 minute:

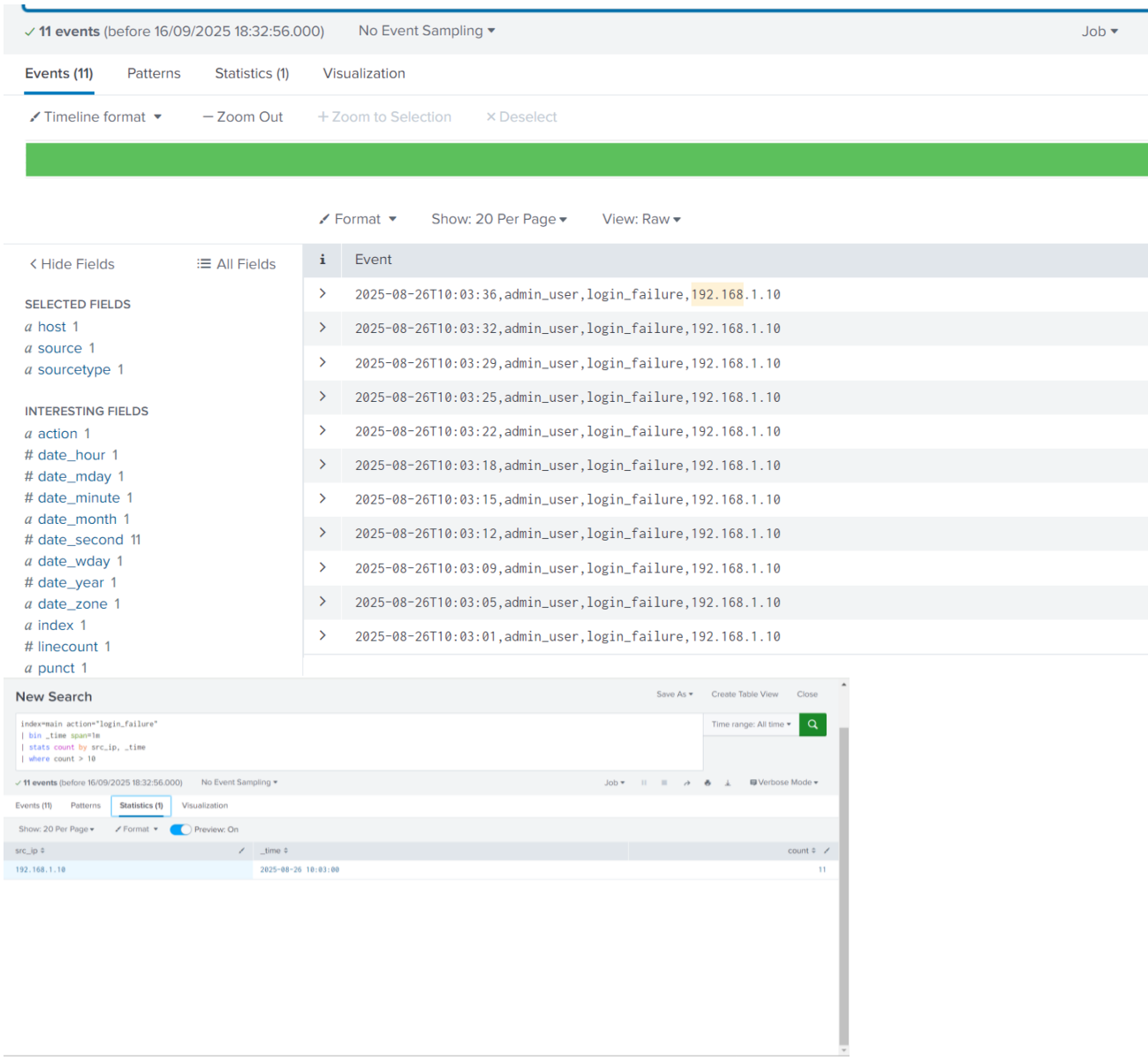
Query:

```
index=main action="login_failure"
| bin _time span=1m
```

| stats count by src_ip, _time
| where count > 10

.





Purpose

This query detects **possible brute-force attacks** by identifying any source IP (src_ip) that generates **more than 10 failed login attempts (login_failure) within a 1-minute interval**.

How It Works

1. **index=main action="login_failure"**
   - Filters events in the main dataset where the action is login_failure.
2. **| bin _time span=1m**
   - Buckets timestamps into **1-minute intervals** to group failures within the same time window.

3. **| stats count by src_ip, _time**
    - Counts the number of failed login attempts for each source IP in each minute.
4. **| where count > 10**
    - Filters to show **only those IPs** that exceed **10 failures in one minute**.

Interpreting from the screenshots)

- **Events Tab:** Shows all 11 raw events for IP 192.168.1.10.
- **Statistics Tab:** Summarizes them as **1 row** with count=11.
    - This means one IP (192.168.1.10) attempted 11 failed logins in a single minute — **strong evidence of a brute-force attempt**.

User-focused view (e.g., admin_user):

Query:

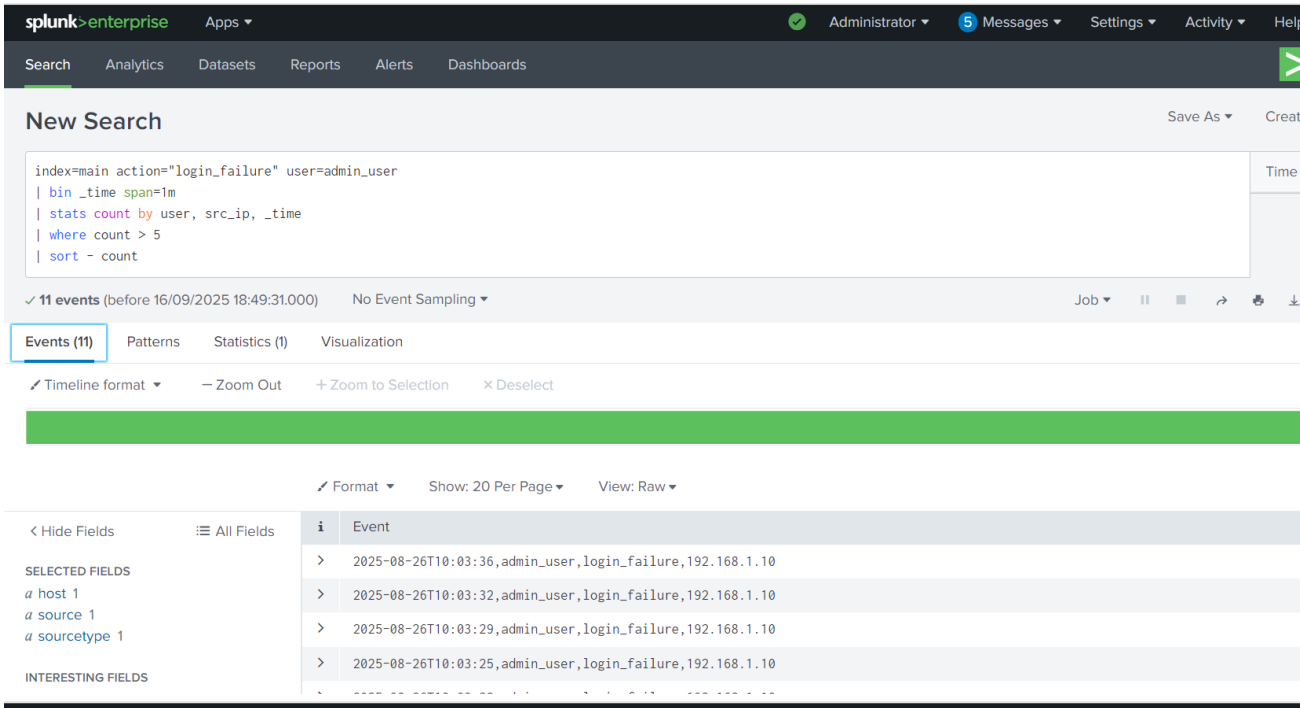
index=main action="login_failure" user=admin_user

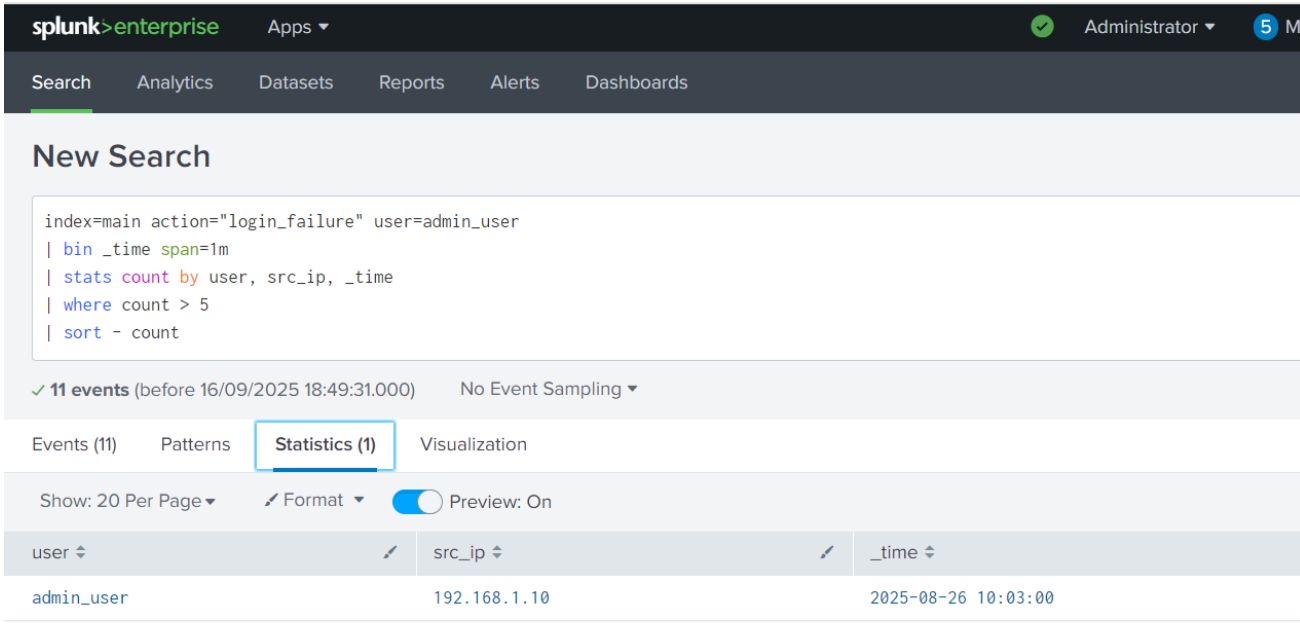
| bin _time span=1m

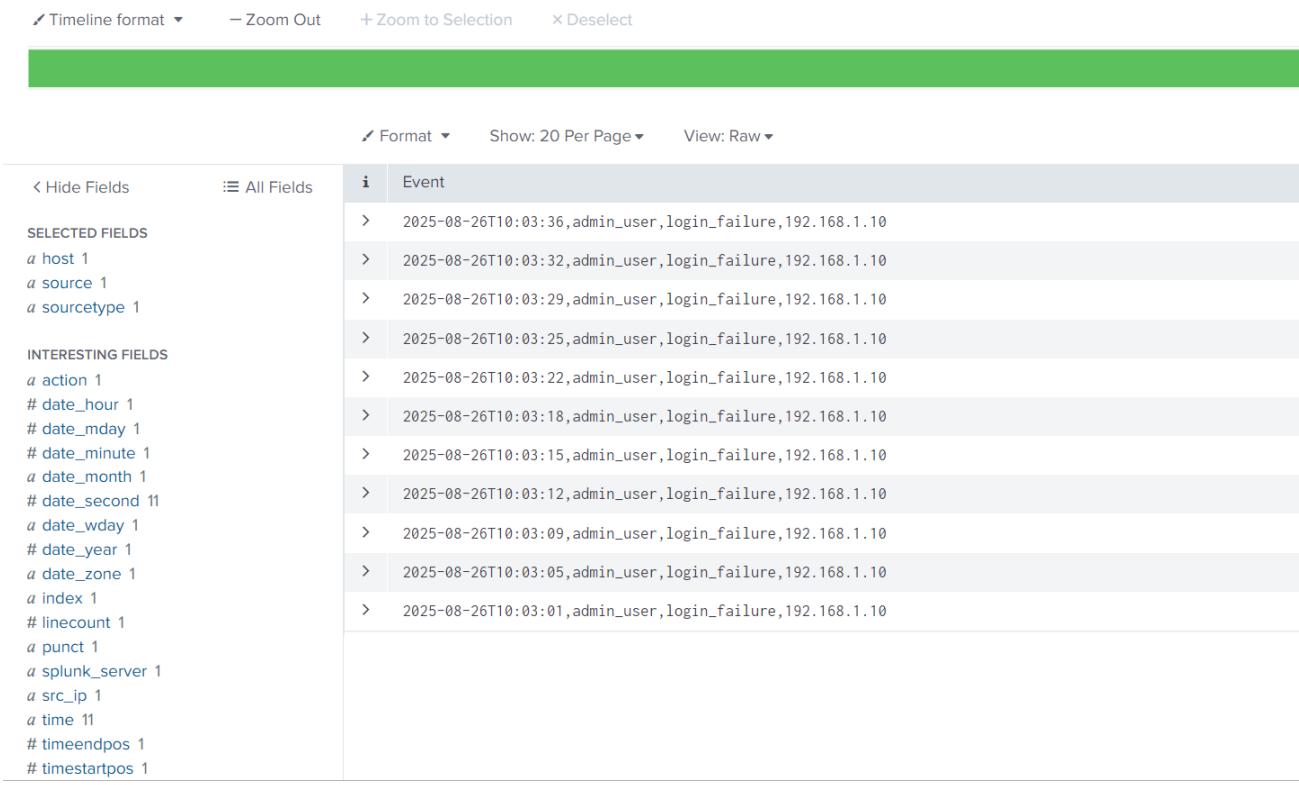
| stats count by user, src_ip, _time

| where count > 5

| sort – count


splunk>enterprise
Apps
Administrator
5 Messages
Settings
Activity
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
Save As
index=main action="login_failure" user=admin_user
| bin _time span=1m
| stats count by user, src_ip, _time
| where count > 5
| sort - count
✓ 11 events (before 16/09/2025 18:49:31.000)
No Event Sampling
Job
Events (11)
Patterns
Statistics (1)
Visualization
Timeline format
– Zoom Out
+ Zoom to Selection
× Deselect
Format
Show: 20 Per Page
View: Raw
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
Event
2025-08-26T10:03:36,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:32,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:29,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:25,admin_user,login_failure,192.168.1.10


splunk>enterprise
Apps
Administrator
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
index=main action="login_failure" user=admin_user
| bin _time span=1m
| stats count by user, src_ip, _time
| where count > 5
| sort - count
✓ 11 events (before 16/09/2025 18:49:31.000)
No Event Sampling
Events (11)
Patterns
Statistics (1)
Visualization
Show: 20 Per Page
Format
Preview: On
user
src_ip
_time
admin_user
192.168.1.10
2025-08-26 10:03:00



Explanation

- **user=admin_user** → Filters to only failed login attempts for the admin_user account.
- **bin _time span=1m** → Groups events into one-minute intervals.
- **stats count by user, src_ip, _time** → Aggregates failed attempts by **user**, **source IP**, and **time**.
- **where count > 5** → Flags more than 5 failures in a minute (adjust based on your environment).
- **sort - count** → Sorts to show the noisiest attackers at the top.

Usage Notes

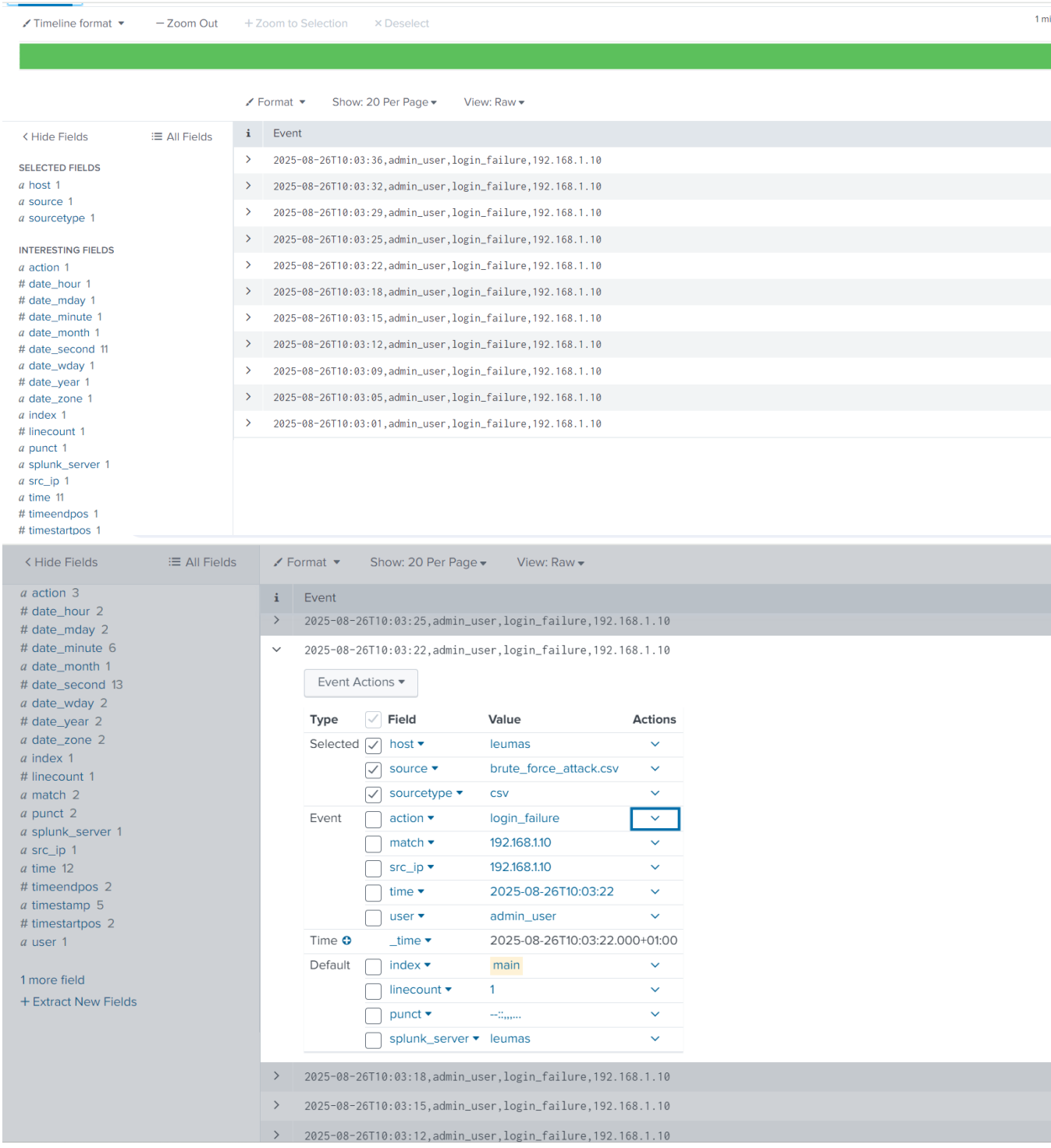
- Use user=* if you want to compare multiple usernames.
- To view both **raw events** and **aggregated stats**, check the **Events** tab and the **Statistics** tab in Splunk.
- Adjust the **threshold** (count > 5) depending on your typical login failure rate.

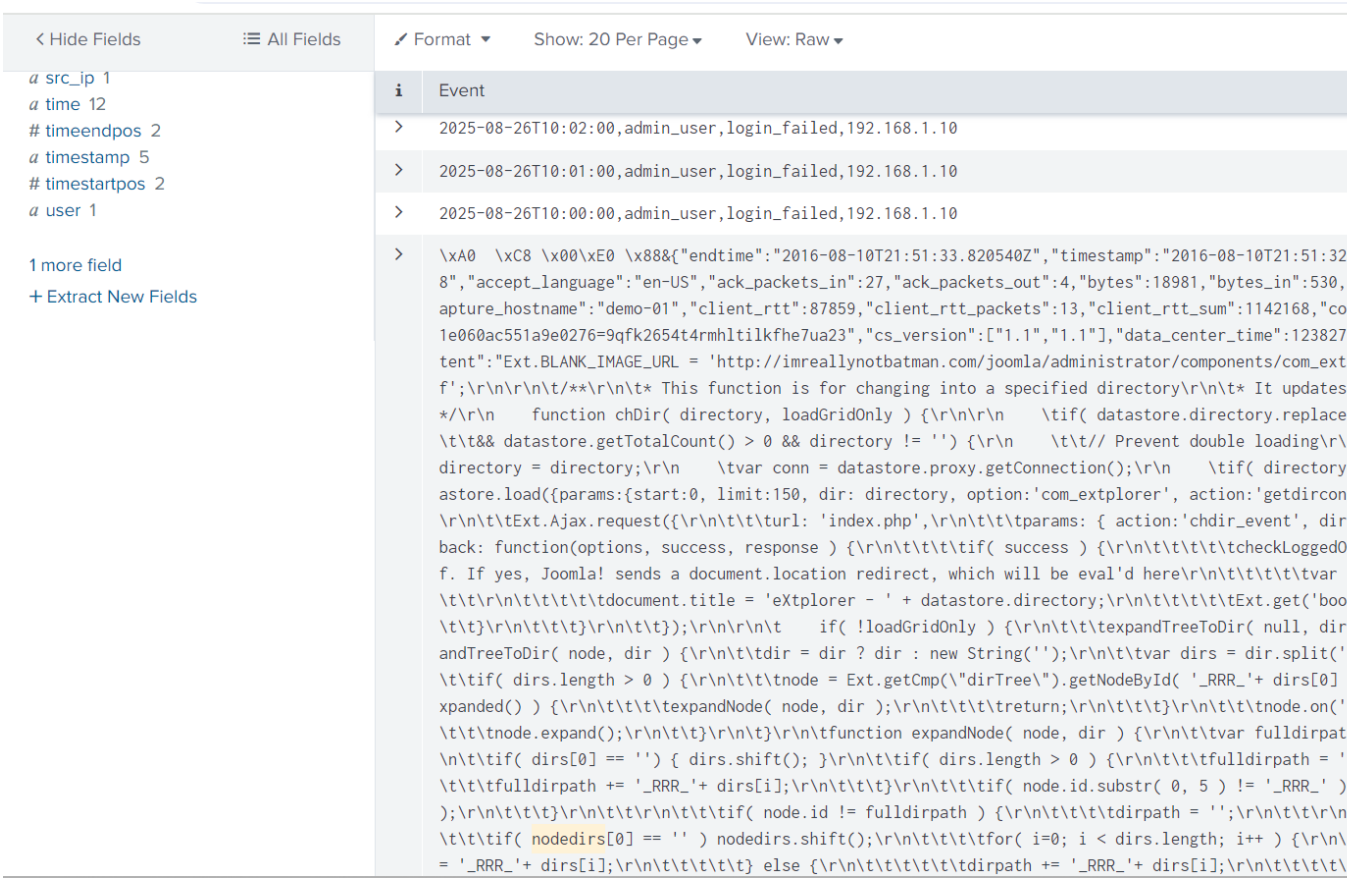
  5) Threat Intelligence Lookup (malicious IP list)

  index=main

  | lookup threat_list.csv ip AS src_ip OUTPUT ip AS match

```
| where isnotnull(match)
```


Timeline format
Zoom Out
Zoom to Selection
Deselect
Format
Show: 20 Per Page
View: Raw
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 1
date_hour 1
date_mday 1
date_minute 1
a date_month 1
date_second 11
a date_wday 1
date_year 1
a date_zone 1
a index 1
linecount 1
a punct 1
a splunk_server 1
a src_ip 1
a time 11
timeendpos 1
timestartpos 1
Event
2025-08-26T10:03:36,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:32,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:29,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:25,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:22,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:18,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:15,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:12,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:09,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:05,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:01,admin_user,login_failure,192.168.1.10
Hide Fields
All Fields
Format
Show: 20 Per Page
View: Raw
a action 3
date_hour 2
date_mday 2
date_minute 6
a date_month 1
date_second 13
a date_wday 2
date_year 2
a date_zone 2
a index 1
linecount 1
a match 2
a punct 2
a splunk_server 1
a src_ip 1
a time 12
timeendpos 2
a timestamp 5
timestartpos 2
a user 1
1 more field
+ Extract New Fields
Event
2025-08-26T10:03:25,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:22,admin_user,login_failure,192.168.1.10
Event Actions
Type
Field
Value
Actions
Selected
host
leumas
source
brute_force_attack.csv
sourcetype
csv
Event
action
login_failure
match
192.168.1.10
src_ip
192.168.1.10
time
2025-08-26T10:03:22
user
admin_user
Time
_time
2025-08-26T10:03:22.000+01:00
Default
index
main
linecount
1
punct
--::,,,...
splunk_server
leumas
2025-08-26T10:03:18,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:15,admin_user,login_failure,192.168.1.10
2025-08-26T10:03:12,admin_user,login_failure,192.168.1.10



Purpose

This search checks network events in your **main** index against a **threat intelligence list** (threat_list.csv) of known malicious IP addresses. It helps detect suspicious activity by highlighting events whose src_ip matches an entry in the threat list.

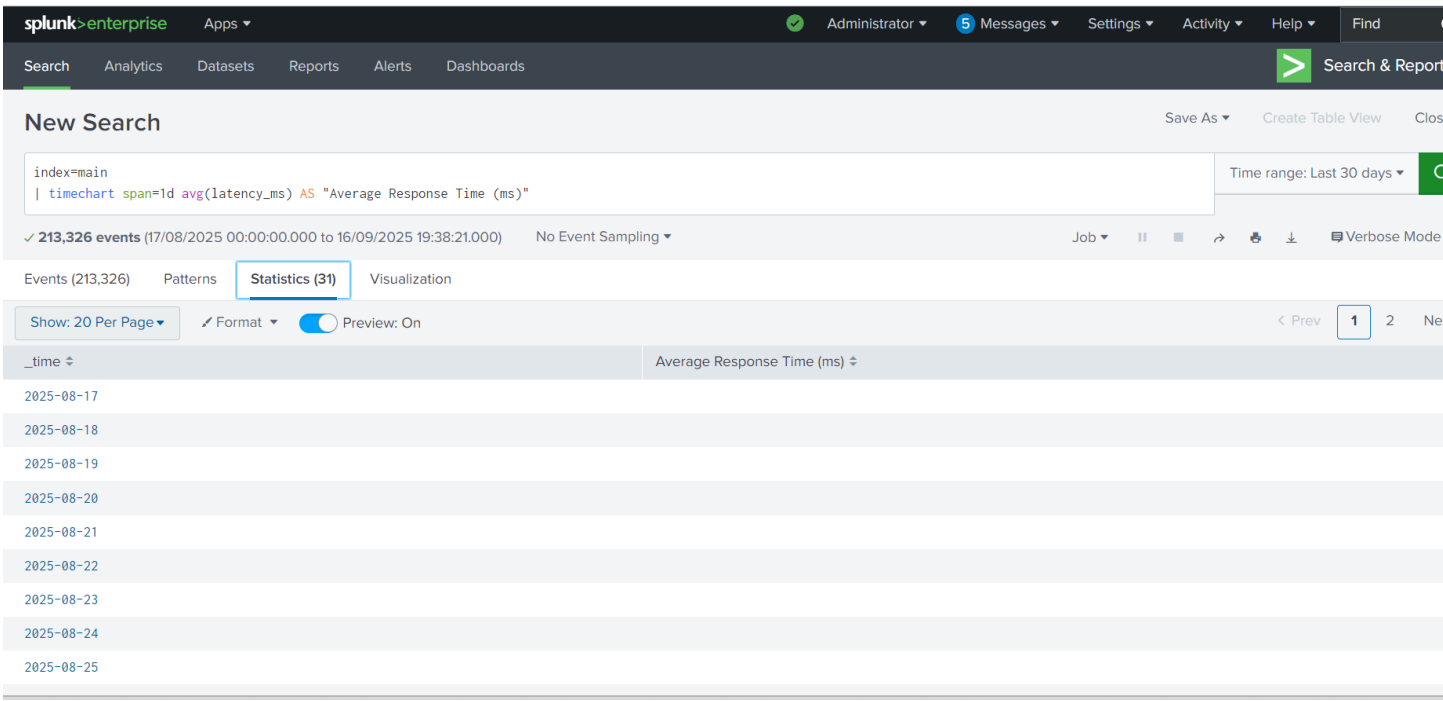
Step-by-Step Breakdown

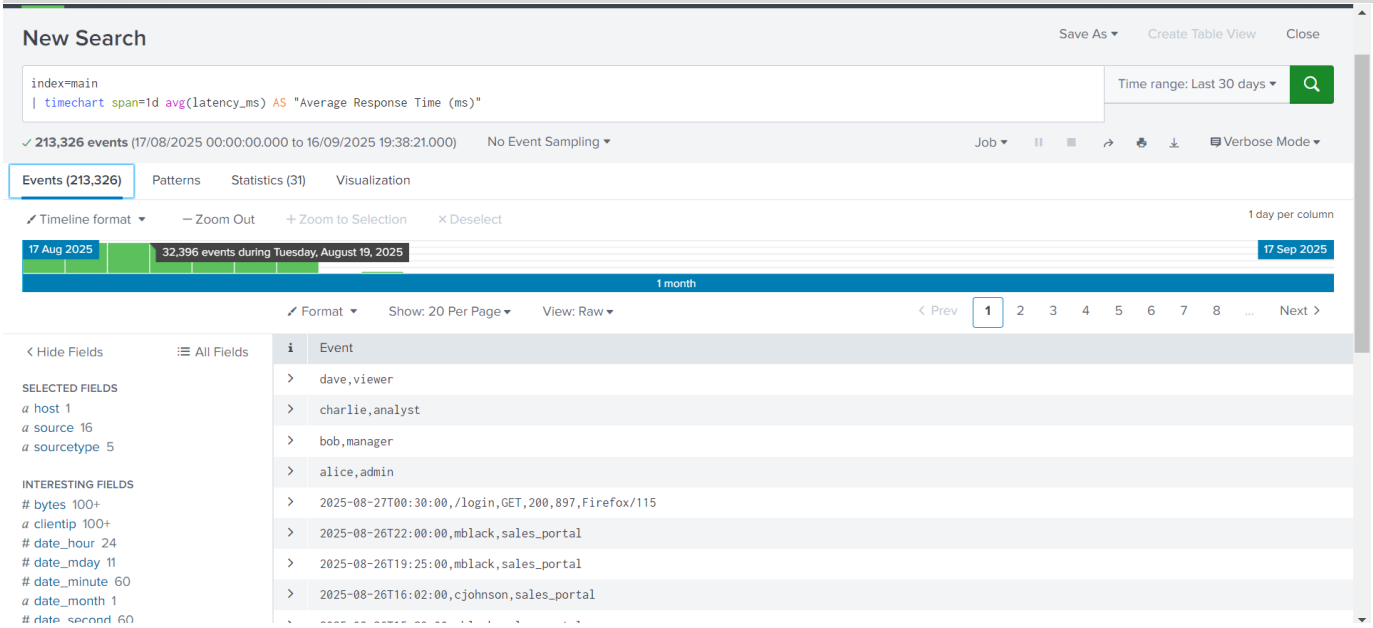
1. **index=main**
   - Searches your Splunk dataset stored in the main index.
2. **lookup threat_list.csv ip AS src_ip OUTPUT ip AS match**
   - Uses threat_list.csv (uploaded as a **lookup table file**) to compare the src_ip field in your events with the ip field in the CSV.
   - If a match is found, a new field called match is added to the event.
3. **where isnotnull(match)**
   - Filters the results to include **only events with a match** in the threat list (ignoring all non-malicious traffic).

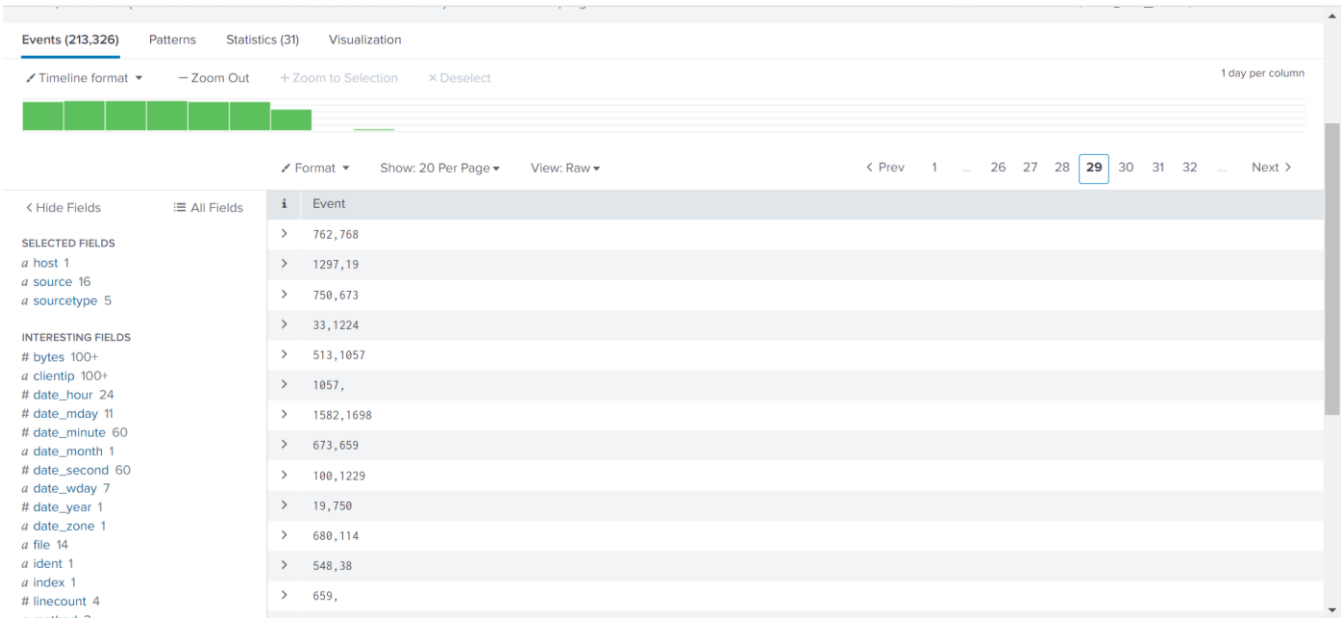
6) Useful visualization queries

Daily average response time (timechart):

```
index=main
| timechart span=1d avg(latency_ms) AS "Average Response Time (ms)"
```


splunk>enterprise
Apps
Administrator
5 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Report
New Search
Save As
Create Table View
Clos
index=main
| timechart span=1d avg(latency_ms) AS "Average Response Time (ms)"
Time range: Last 30 days
213,326 events (17/08/2025 00:00:00.000 to 16/09/2025 19:38:21.000)
No Event Sampling
Job
Verbose Mode
Events (213,326)
Patterns
Statistics (31)
Visualization
Show: 20 Per Page
Format
Preview: On
Prev
1
2
Ne
_time
Average Response Time (ms)
2025-08-17
2025-08-18
2025-08-19
2025-08-20
2025-08-21
2025-08-22
2025-08-23
2025-08-24
2025-08-25


New Search
Save As
Create Table View
Close
index=main
| timechart span=1d avg(latency_ms) AS "Average Response Time (ms)"
Time range: Last 30 days
213,326 events (17/08/2025 00:00:00.000 to 16/09/2025 19:38:21.000)
No Event Sampling
Job
Verbose Mode
Events (213,326)
Patterns
Statistics (31)
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 day per column
17 Aug 2025
32,396 events during Tuesday, August 19, 2025
17 Sep 2025
1 month
Format
Show: 20 Per Page
View: Raw
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 16
a sourcetype 5
INTERESTING FIELDS
bytes 100+
a clientip 100+
date_hour 24
date_mday 11
date_minute 60
a date_month 1
date_second 60
Event
dave,viewer
charlie,analyst
bob,manager
alice,admin
2025-08-27T00:30:00,/login,GET,200,897,Firefox/115
2025-08-26T22:00:00,mblack,sales_portal
2025-08-26T19:25:00,mblack,sales_portal
2025-08-26T16:02:00,cjohnson,sales_portal



Documentation Note

Purpose:
Visualize the **daily average response time** to monitor performance trends.

Steps:

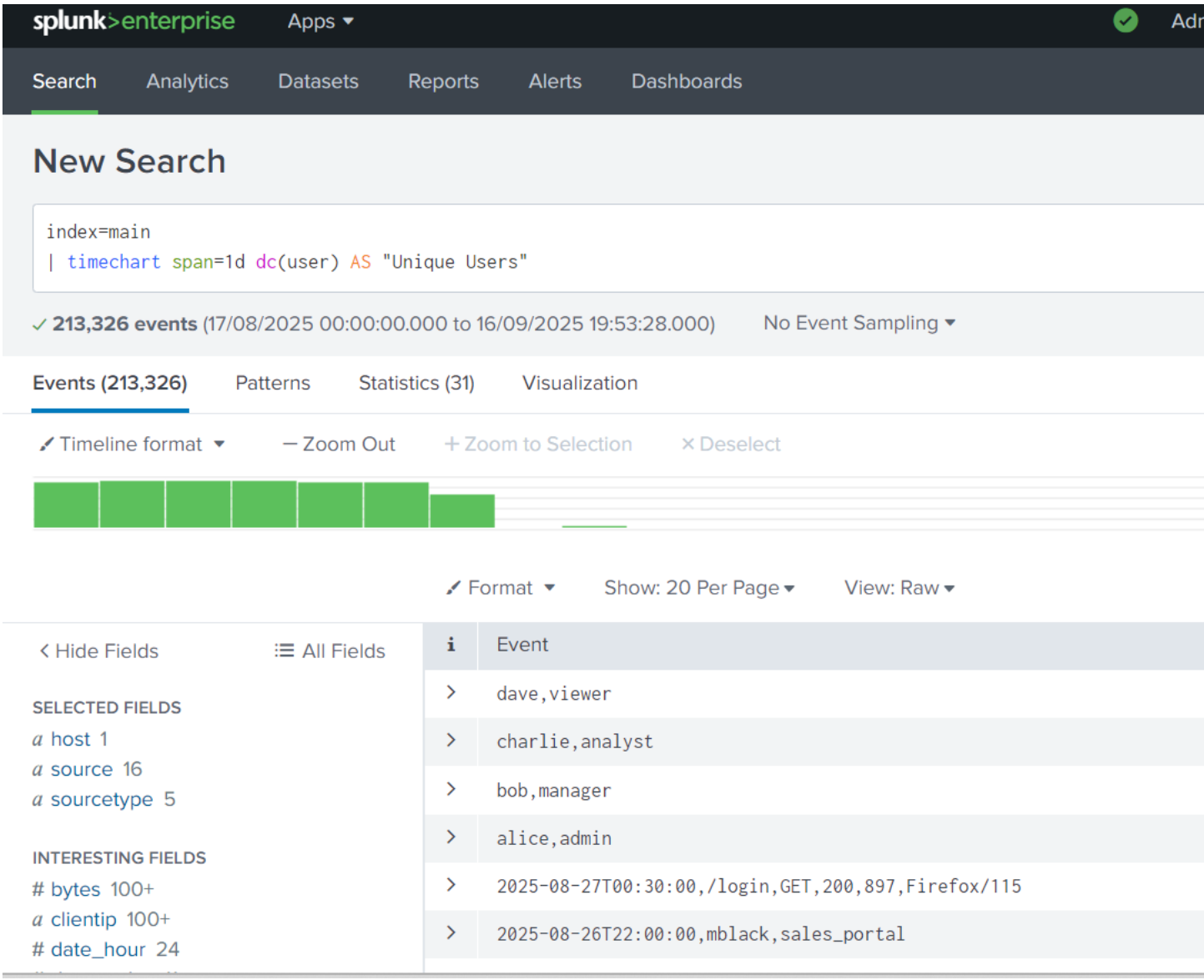
- Use timechart to aggregate values into daily buckets (span=1d).
- Use avg() to calculate average latency.
- Label the output for clarity (AS "Average Response Time (ms)").

Use Case:
Operations teams can quickly identify latency spikes or degradations in service performance over time.

Unique users per day (dashboard-ready):

index=main

| timechart span=1d dc(user) AS "Unique Users"


splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
index=main
| timechart span=1d dc(user) AS "Unique Users"
213,326 events (17/08/2025 00:00:00.000 to 16/09/2025 19:53:28.000)
No Event Sampling
Events (213,326)
Patterns
Statistics (31)
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
Format
Show: 20 Per Page
View: Raw
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 16
a sourcetype 5
INTERESTING FIELDS
bytes 100+
a clientip 100+
date_hour 24
Event
dave,viewer
charlie,analyst
bob,manager
alice,admin
2025-08-27T00:30:00,/login,GET,200,897,Firefox/115
2025-08-26T22:00:00,mblack,sales_portal

New Search

```
index=main
| timechart span=1d dc(user) AS "Unique Users"
```

✓ **213,326 events** (17/08/2025 00:00:00.000 to 16/09/2025 19:53:28.000) No Event Sampling

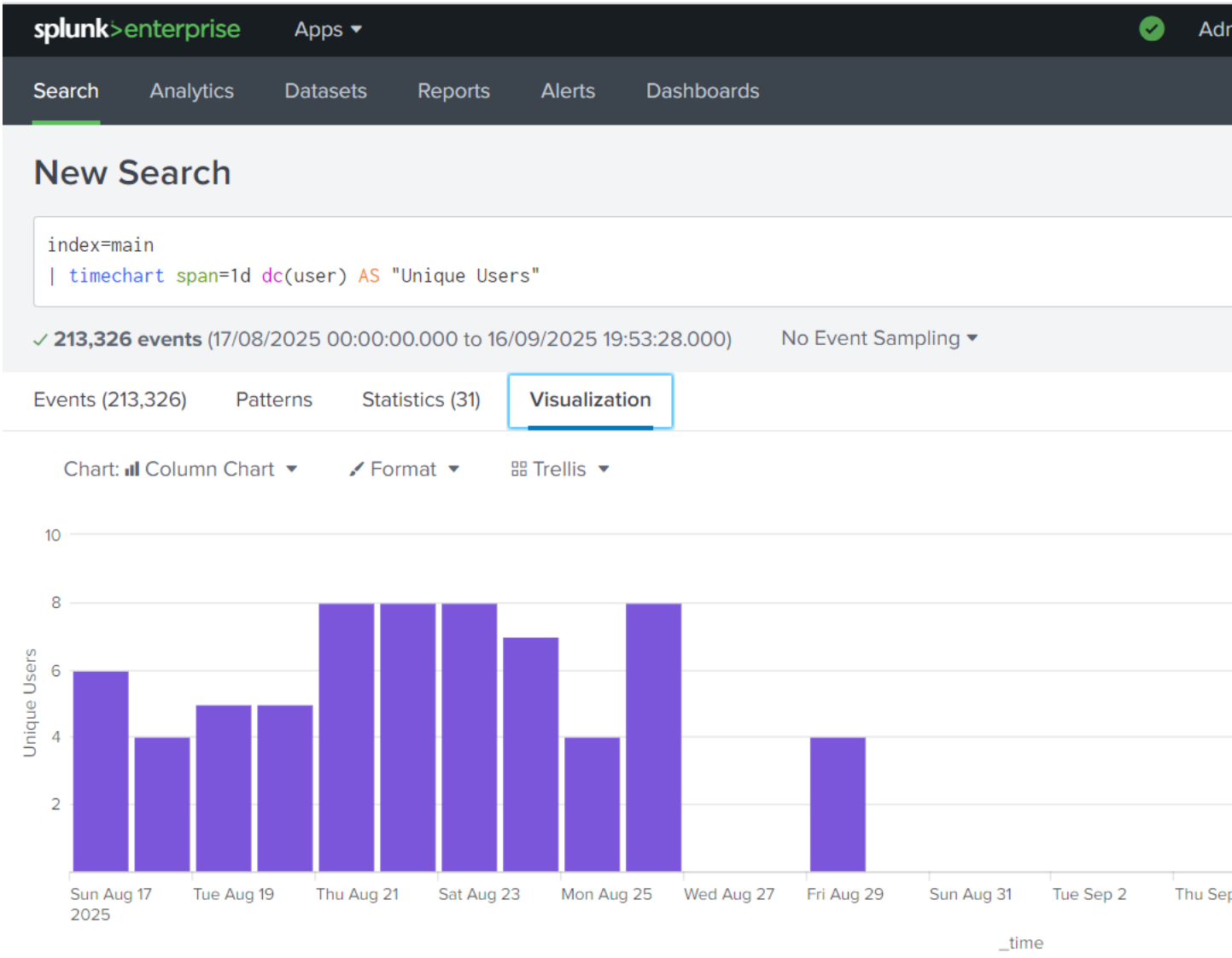
Events (213,326) Patterns **Statistics (31)** Visualization

Show: 20 Per Page Format Preview: On

_time
2025-08-17
2025-08-18
2025-08-19
2025-08-20
2025-08-21
2025-08-22
2025-08-23
2025-08-24
2025-08-25
2025-08-26
2025-08-27
2025-08-28
2025-08-29

Show: 20 Per Page | Format | Preview: On

_time
2025-08-18
2025-08-19
2025-08-20
2025-08-21
2025-08-22
2025-08-23
2025-08-24
2025-08-25
2025-08-26
2025-08-27
2025-08-28
2025-08-29
2025-08-30
2025-08-31
2025-09-01
2025-09-02
2025-09-03
2025-09-04



Explanation

- **timechart span=1d** → Buckets events by day.
- **dc(user)** → Counts **distinct (unique)** values of the user field for each day.
- **AS "Unique Users"** → Renames the column for dashboard display clarity.

Usage Notes

1. **Field check** – Ensure your dataset includes a field called user. If not, replace user with the actual username field (username, account, etc.).
2. **Time range** – Use a broad range (e.g., *Last 30 days*) for trends.
3. **Dashboard panel** –
    - In Splunk, click **Save As → Dashboard Panel**.

- Choose a dashboard and panel type (e.g., **Line Chart** or **Area Chart**) for a visual trend of active users over time.

Purpose:
Track the number of unique users accessing the system daily to monitor usage patterns or potential anomalies.

Use Case:

4. Identify unusual spikes in new user activity.
5. Monitor service adoption or user engagement trends.
6. Detect possible credential-sharing or security incidents if numbers deviate sharply.

-