Splunk

```
# list all indexes, cmdline: splunk list index
| eventcount summarize=false index=* | dedup index | fields index

sourcetype=access_combined error | top 5 uri

[+|-]<integer><unit>@<snap_time_ unit>

"error earliest=-1d@d latest=h@h"

#subsearch
sourcetype=syslog [ search login error | return 1 user ]


source="/var/log/myapp/access.log" status=404

host="myblog" source="/var/log/syslog" Fatal

index=* OR index=_* sourcetype=generic_logs | search Cybersecurity | head
10000

#ipv4
| regex !="^\d{1,3}.\d{1,3}\.\d{1,3}\.\d{1,3}"

#rex -> extract
source="email_dump.txt" | rex field=_raw "From: <(?<from>.*)> To:
<(?<to>.*)>"
```

chart/ timechart

Returns results in a tabular output for (time-series) charting.

dedup

Removes subsequent results that match a specified criterion.

eval

Calculates an expression. See COMMON EVAL FUNCTIONS.

fields

Removes fields from search results.

head/tail

Returns the first/last N results.

lookup

Adds field values from an external source.

rename

Renames a field. Use wildcards to specify multiple fields.

rex

Specifies regular expression named groups to extract fields.

search

Filters results to those that match the search expression.

sort

Sorts the search results by the specified fields.

stats

Provides statistics, grouped optionally by fields. See COMMON STATS FUNCTIONS.

mstats

Similar to stats but used on metrics instead of events.

table

Specifies fields to keep in the result set. Retains data in tabular format.

top/rare

Displays the most/least common values of a field.

transaction

Groups search results into transactions.

where

Filters search results using eval expressions. Used to compare two different fields.