Sumo logic Searching

gist.github.com/dariatrainor/2e991b90f6315c172acae688c2b39de2

262588213843476

```
Boolean logic and *: _sourceCategory=Labs/Apache/Access AND (Error OR check*)
Live Tail sessions support wildcards searches


Conditional operators allow you to do if/then operations

_sourceCategory=Labs/Apache/Access
| parse "HTTP/1.1\" * " as status_code
| if(status_code=200, 1, 0) as successes
| if(status_code=404, 1, 0) as client_errors
| sum(successes) as success_cnt, sum(client_errors) as client_errors_cnt
```