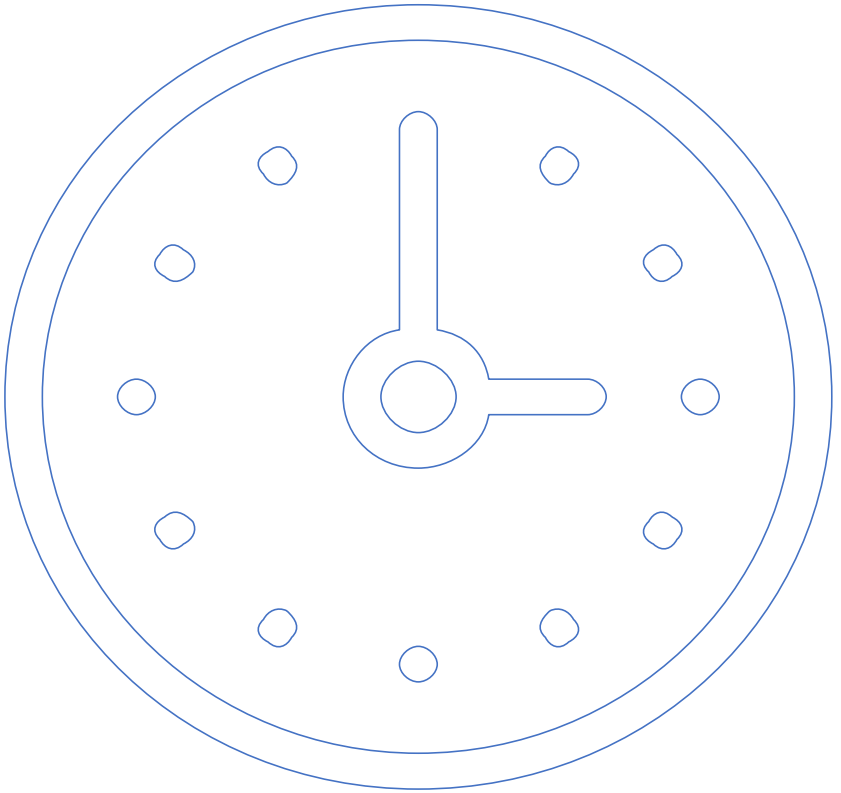
# Dados temporais

Elasticsearch pode agrupar campos com datas e hora e sabe as regras do tempo/calendário. Você pode, por exemplo, agrupar por ano ou mês.



Sundog Education

Coralogix

PROF. FERNANDO AMARAL

# Dividir acessos ao site por hora

```
curl -XGET '127.0.0.1:9200/kafka-logs/_search?size=0&pretty' -d ‘
{
        "aggs" : {
                "timestamp": {
                        "date_histogram": {
                                "field": "@timestamp",
                                "interval": "hour"
                        }
                }
        }
}'
```

# Quando o Google acessa minha página?

```
curl -XGET '127.0.0.1:9200/kafka-logs/_search?size=0&pretty' -d ‘
{
        "query" : {
                "match": {
                        "agent": "Googlebot"
                }
        },
        "aggs" : {
                “timestamp": {
                        "date_histogram": {
                                "field": "@timestamp",
                                "interval": "hour"
                        }
                }
        }
}'
```

Sundog Education  Coralogix  PROF. FERNANDO AMARAL


Sundog
Education

Coralogix

PROF.
FERNANDO
AMARAL