Kibana

Query Basics

`@timestamp >= “2023-01-01”`	Timestamp
(X AND Y) OR Z	

Lucene

1. Turn off KQL to use the Lucene query syntax

Fuzzy

`fu~~y`	fuzzy operator
`“server error”~4`	“slop value” → server and error up to 4 positions apart

Regex

```
Event_Type: /.*/
Description: /(s|m).*/
```

EQL

```
file where host.os.type == "linux" and
 event.action in ("rename", "creation") and
 file.path in (
   "/etc/crontab",
   "/etc/cron.allow",
   "/etc/cron.deny"
 )
```

Quicksheets

Http/s

```
client.ip
user.agent
http.request.method
url.path
http.response.status_code
```