Kibana

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

Regex

1. Turn off KQL to use the Lucene query syntax

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