Logging in 

with the 

Philipp Krenn **@xeraa**

Production

elastic

@xeraa

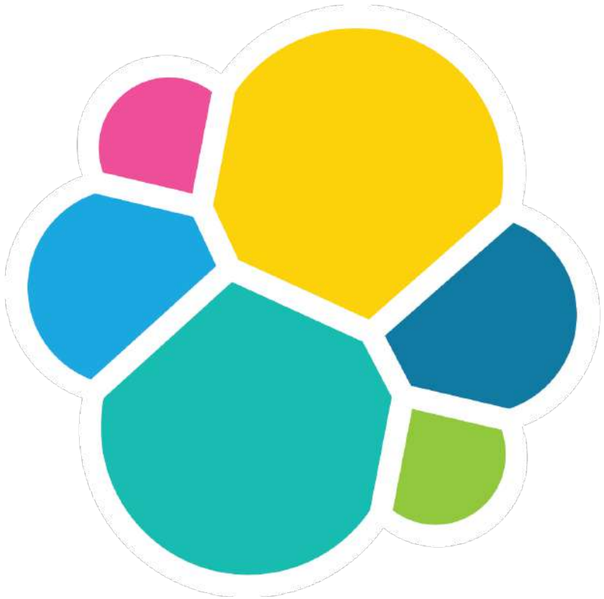
Logs

Timestamp, Log Level, Message, Service

SSH + tail

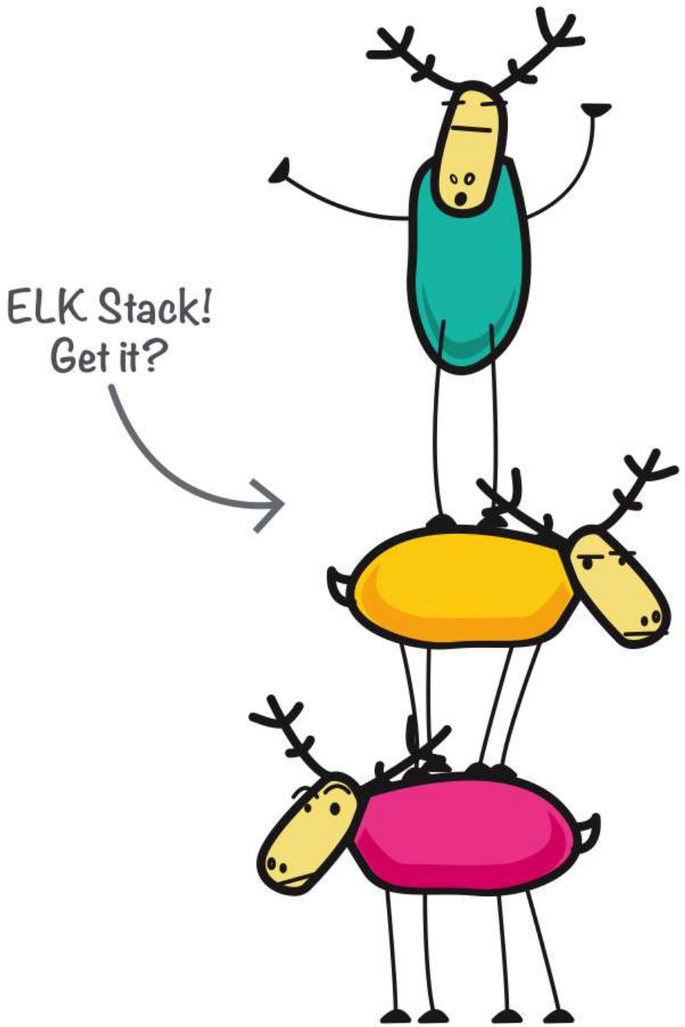

me looking
for the bug
7.2 GB
of log file


So many possibilities!



elastic

Developer 🥑



E Elasticsearch

L Logstash

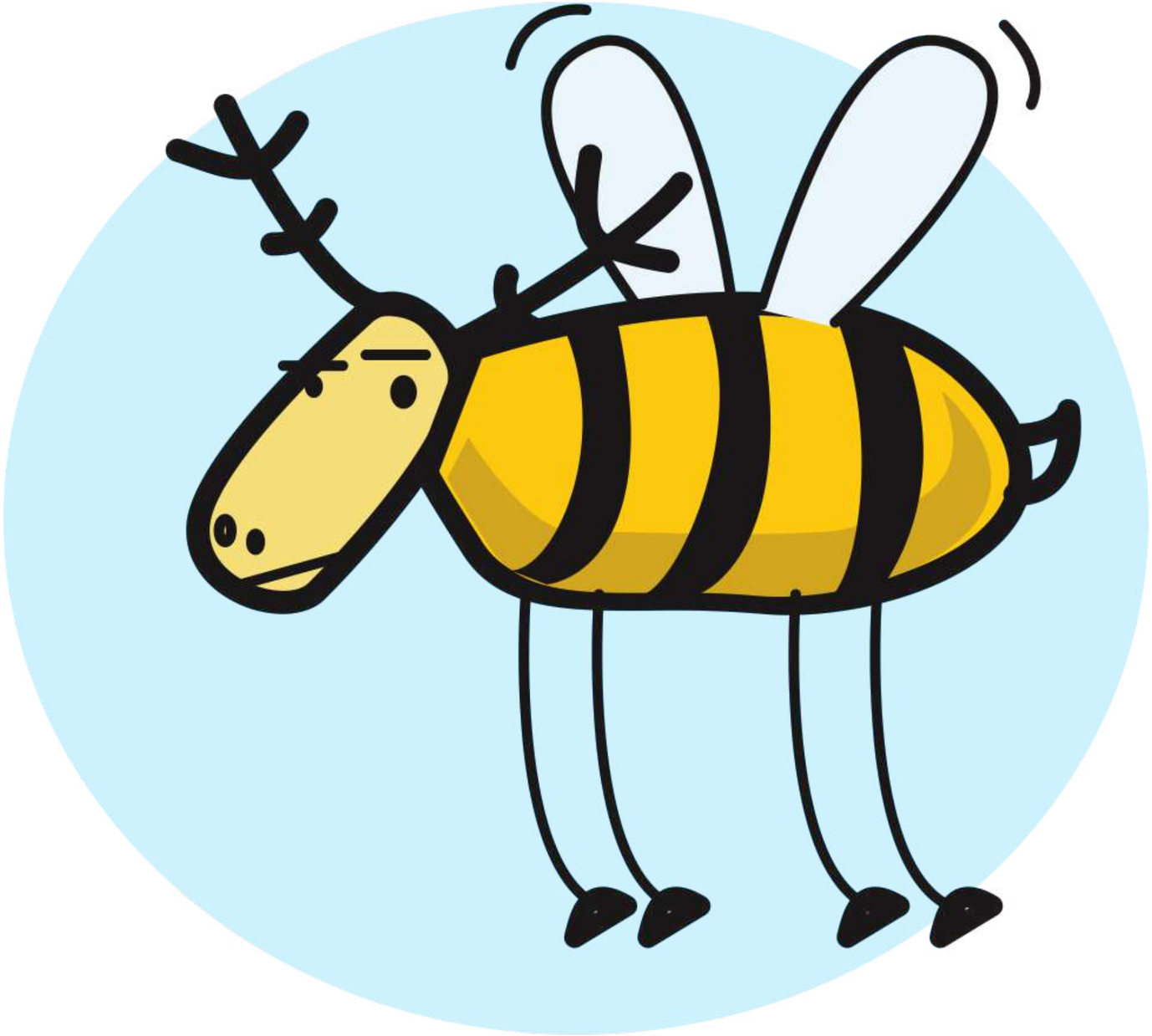
K Kibana

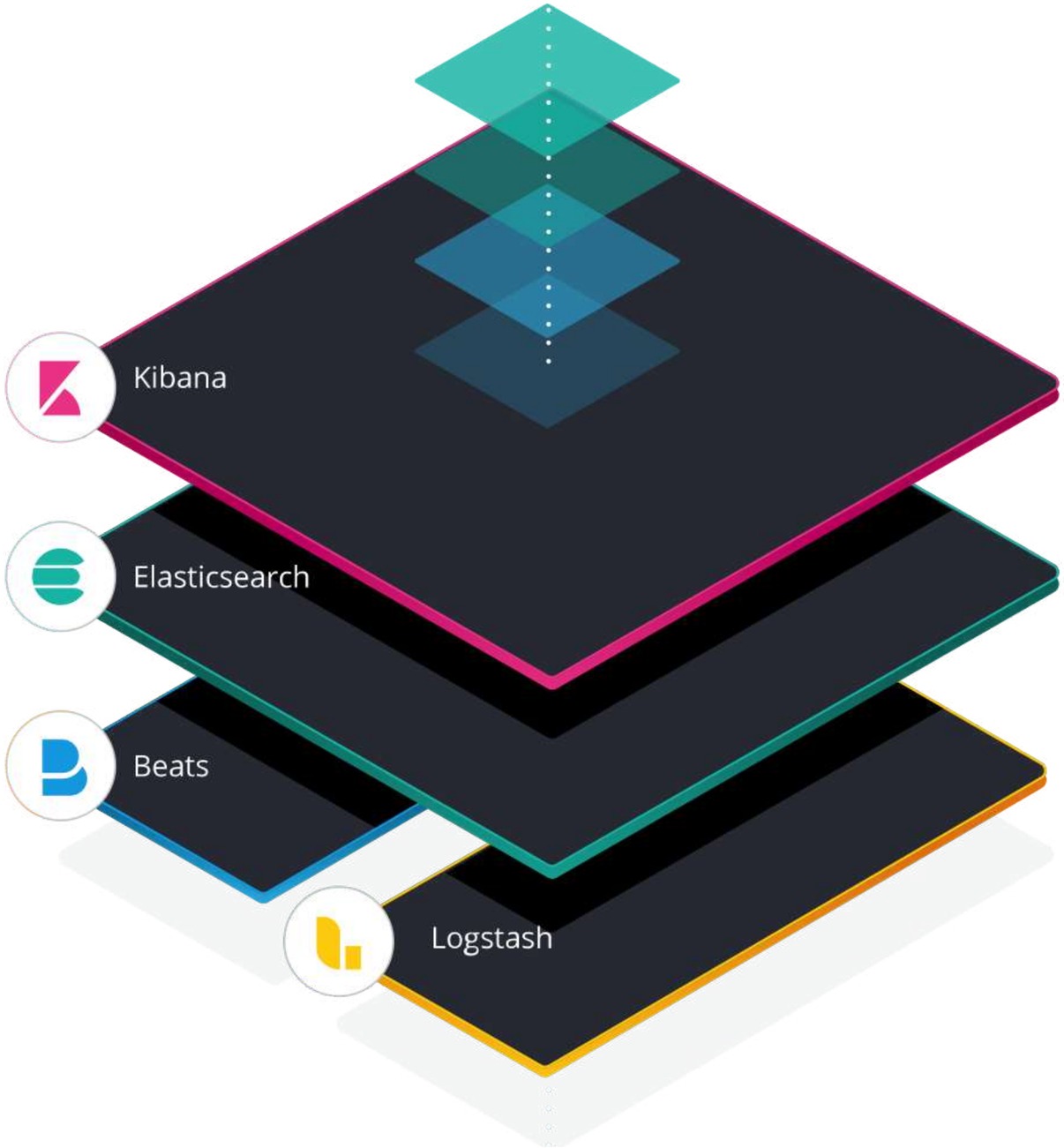
Elasticsearch

Speed, Relevance, Scale

elastic

@xeraa





elastic

@xeraa

Log Lifecycle

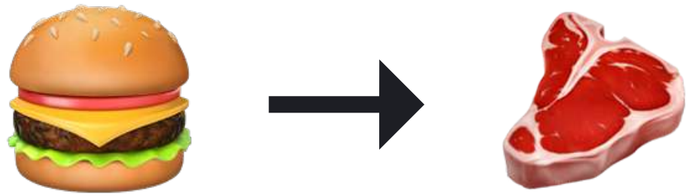
elastic

@xeraa

The plural of regex is regrets

— https://twitter.com/ifosteve/status/1190348262500421634

Multiline Logs



elastic

@xeraa

~~Send Directly~~

logging

ECS

Elastic Common Schema

https://www.elastic.co/guide/en/ecs/current/ecs-reference.html

Field	Description	Level
log.level	Original log level of the log event. If the source of the event provides a log level or textual severity, this is the one that goes in `log.level`. If your source doesn't specify one, you may put your event transport's severity here (e.g. Syslog severity). Some examples are `warn`, `err`, `i`, `informational`. type: keyword example: `error`	core
log.logger	The name of the logger inside an application. This is usually the name of the class which initialized the logger, or can be a custom name. type: keyword example: `org.elasticsearch.bootstrap.Bootstrap`	core
log.origin.file.line	The line number of the file containing the source code which originated the log event. type: integer	extended

ECS Java Logs

Logback, Log4j2, Log4j, JUL

https://github.com/elastic/ecs-logging-java

ECS Java Logs

Consistency, no dependencies, low latency, garbage free

elastic

@xeraa

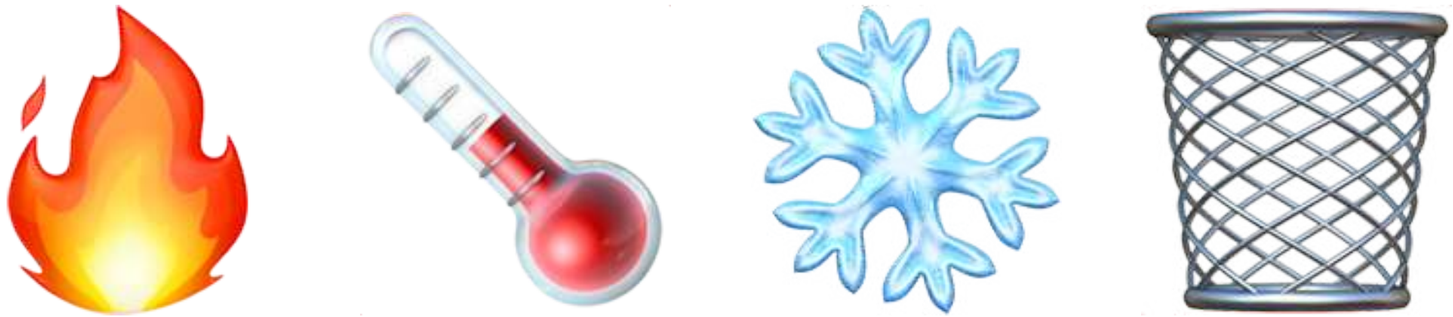
Demo

ILM

Index Lifecycle Management

elastic

@xeraa



Conclusion

Structure

How & Why

Alternative Loggers

https://github.com/vy/log4j2-logstash-layout

https://github.com/logstash/logstash-logback-encoder

Elastic Stack

Free & Open

elastic

@xeraa

Logging in 

with the 

Philipp Krenn **@xeraa**