

Logging in



with the



Philipp Krenn

@xeraa




Production



Logs

Timestamp, Log Level, Message, Service

SSH + tail

A large, rusted metal structure, possibly a ship's hull, is shown in a dark, blue-tinted environment. A bright light source is visible in the background, creating a strong glow and casting shadows on the structure. The structure has a complex, multi-layered appearance with various pipes, beams, and sections.

me looking
for the bug

7.2 GB
of log file

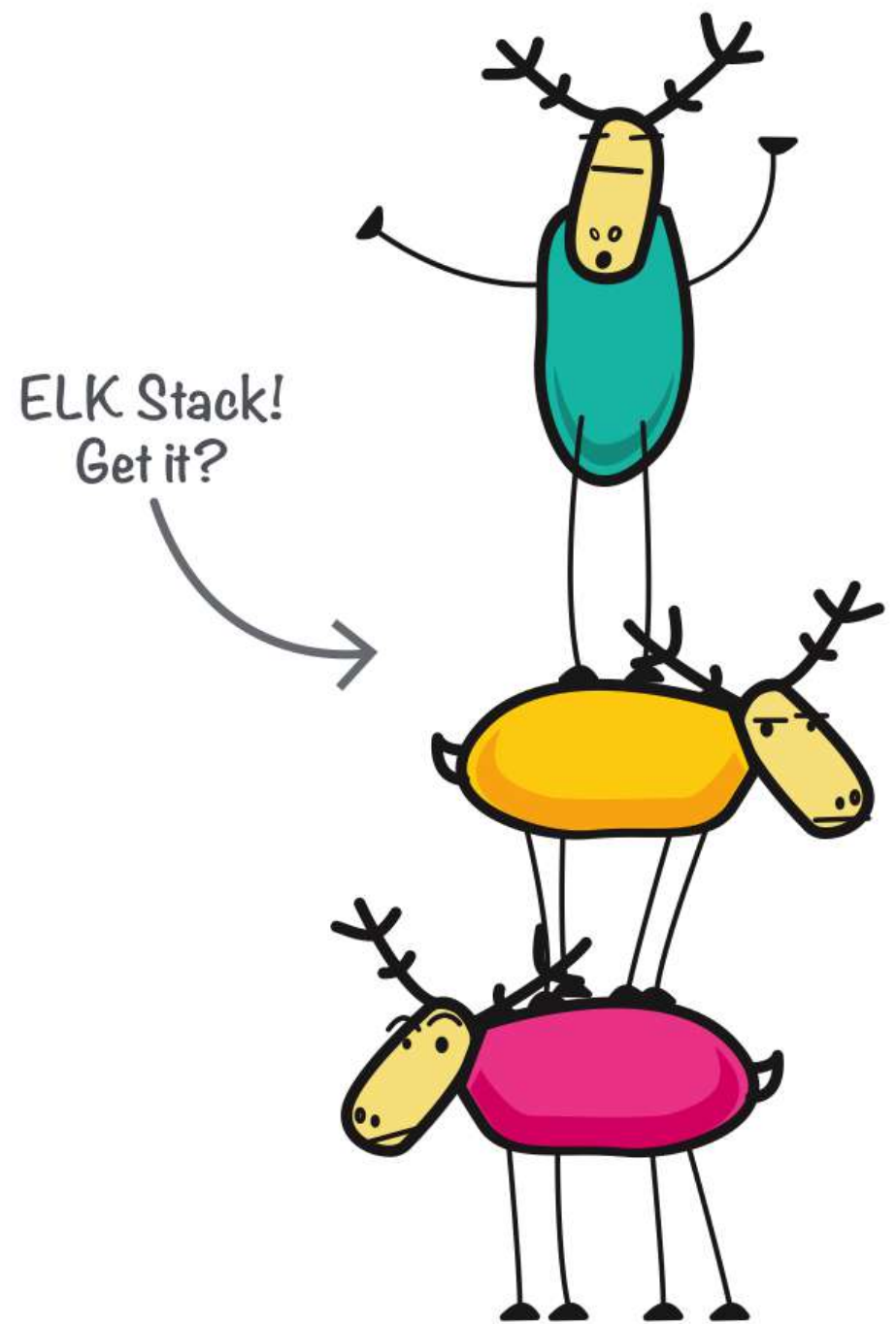
A cartoon illustration showing three people in a room looking at a glowing green cube on a yellow table. On the left, a woman with orange hair in a pink tank top looks surprised. In the center, a man with brown hair in a green polo shirt looks shocked. On the right, a woman with blonde hair in a red dress looks amazed. The cube is dark green with glowing green circles on its faces. The background includes a doorway, a framed picture on the wall, and a kitchen counter with a teapot.

So many possibilities!



elastic

Developer 🥑



ELK Stack!
Get it?

E Elasticsearch

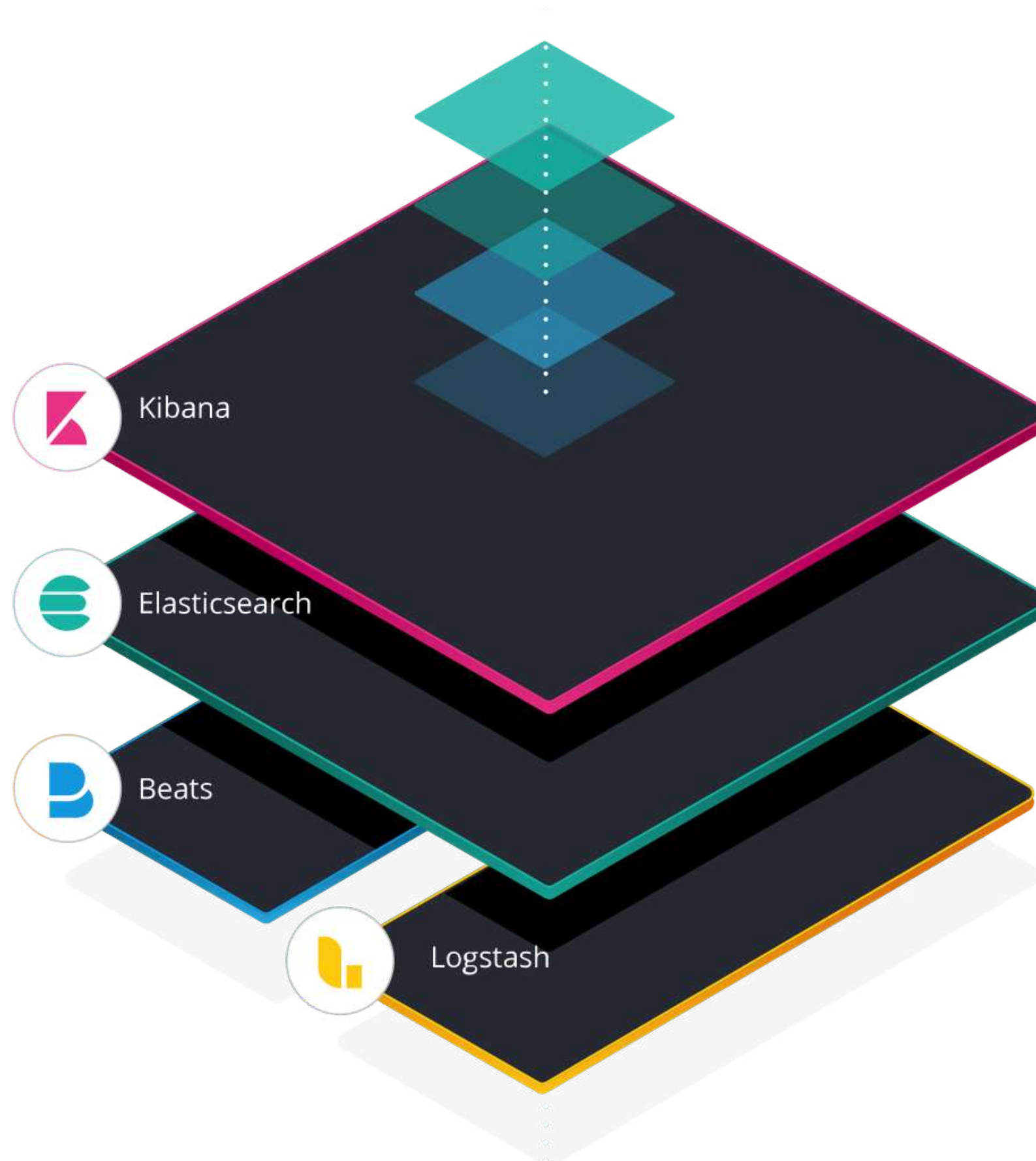
L Logstash

K Kibana

Elasticsearch

Speed, Relevance, Scale





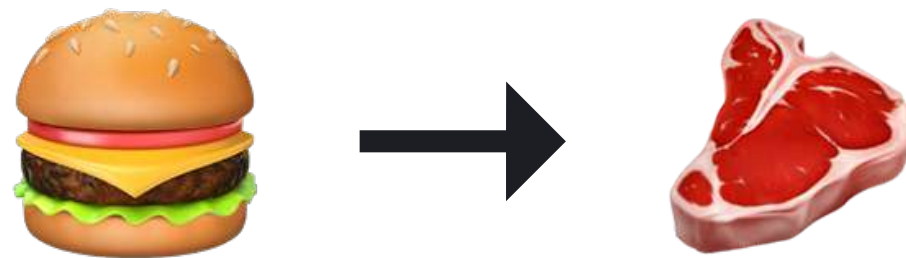
Log Lifecycle



The plural of regex is regrets

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

Multiline Logs



~~Send Directly~~



logging

ECS

Elastic Common Schema

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

| Field | Description | Level |
|----------------------|---|----------|
| log.level | <p>Original log level of the log event.</p> <p>If the source of the event provides a log level or textual severity, this is the one that goes in <code>log.level</code>. If your source doesn't specify one, you may put your event transport's severity here (e.g. Syslog severity).</p> <p>Some examples are <code>warn</code>, <code>err</code>, <code>i</code>, <code>informational</code>.</p> <p>type: keyword</p> <p>example: <code>error</code></p> | core |
| log.logger | <p>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.</p> <p>type: keyword</p> <p>example: <code>org.elasticsearch.bootstrap.Bootstrap</code></p> | core |
| log.origin.file.line | <p>The line number of the file containing the source code which originated the log event.</p> <p>type: integer</p> | 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**

Demo

ILM

Index Lifecycle Management



Conclusion

Structure

How & Why

Alternative Loggers

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

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

Elastic Stack

Free & Open

Logging in



with the



Philipp Krenn

@xeraa

