ELK Stack on Docker within minutes

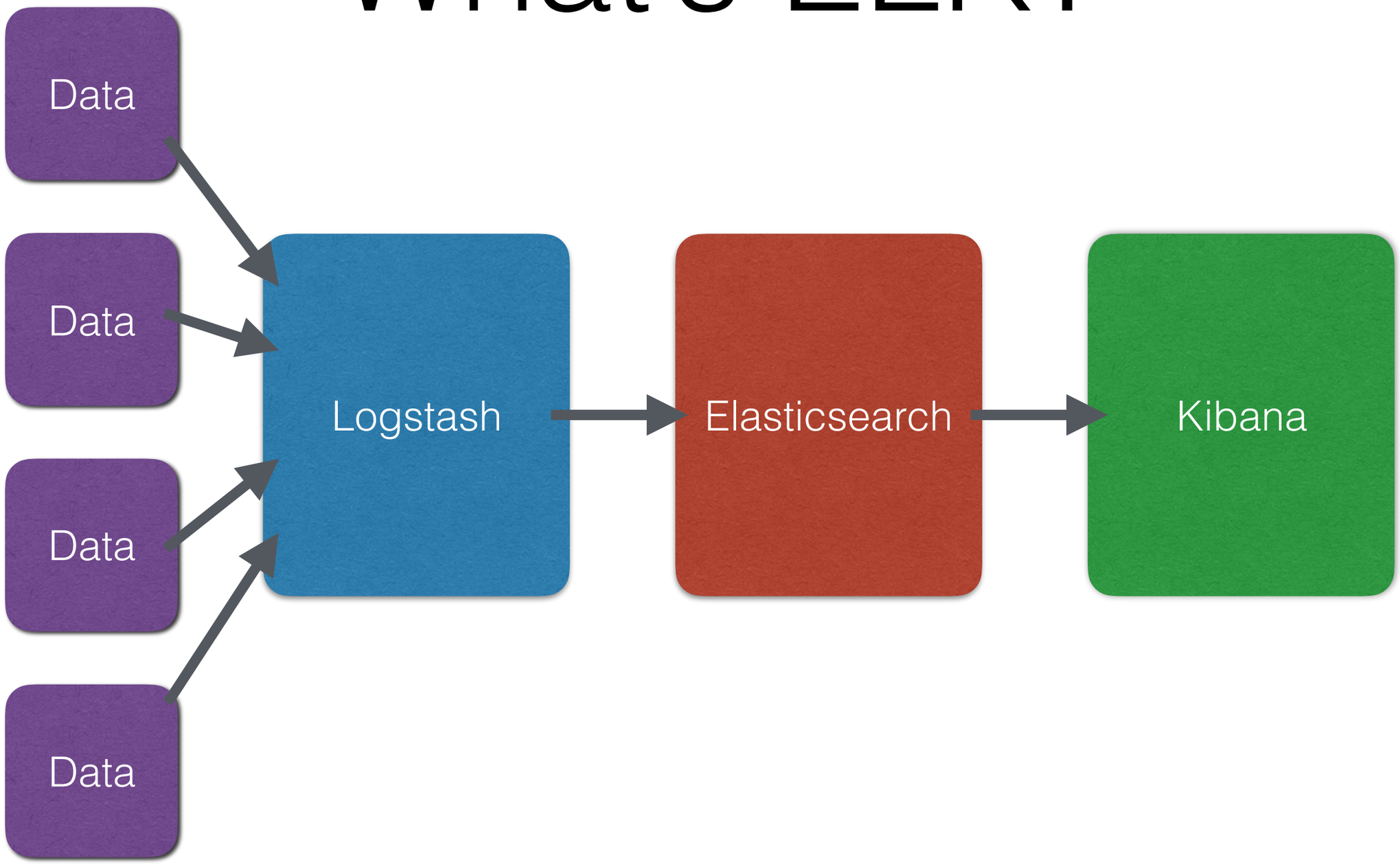
Bernhard Woditschka

What’s ELK?

- Elasticsearch - Search and analyze data
- Logstash - Collect, enrich, and transport data
- Kibana - Explore and visualise

- www.elastic.co

What's ELK?



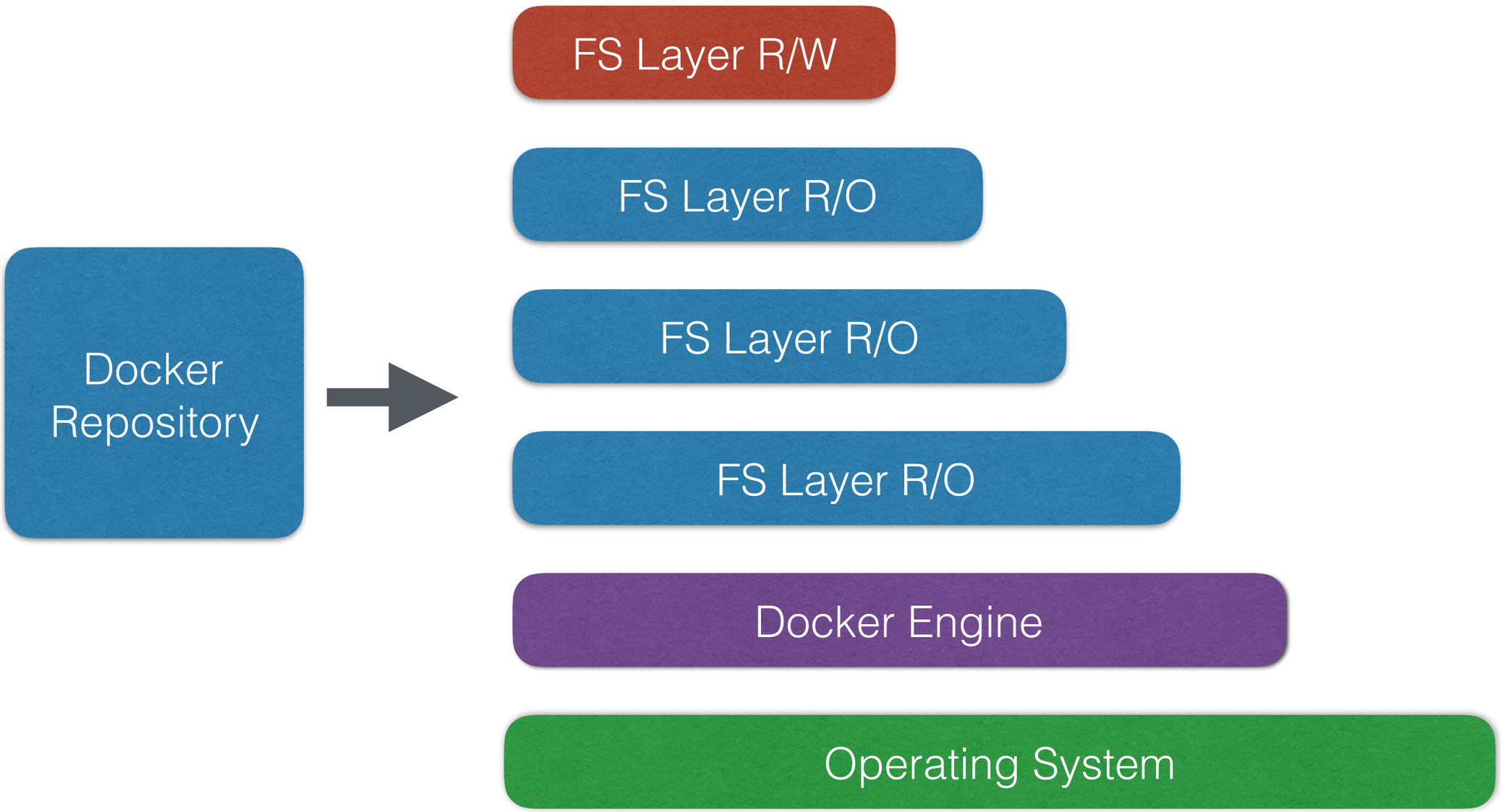
What’s Docker?

- High level API lightweight Linux containers
- Package format with all dependencies
- Layerd File System
- https://www.docker.com/

What’s Docker?

- Docker Engine
- Docker CLI
- Docker Repository
- https://www.docker.com/

What's Docker?



Snowflake / Phoenix Server

- Install Java, download packages, configure

  https://www.elastic.co/products

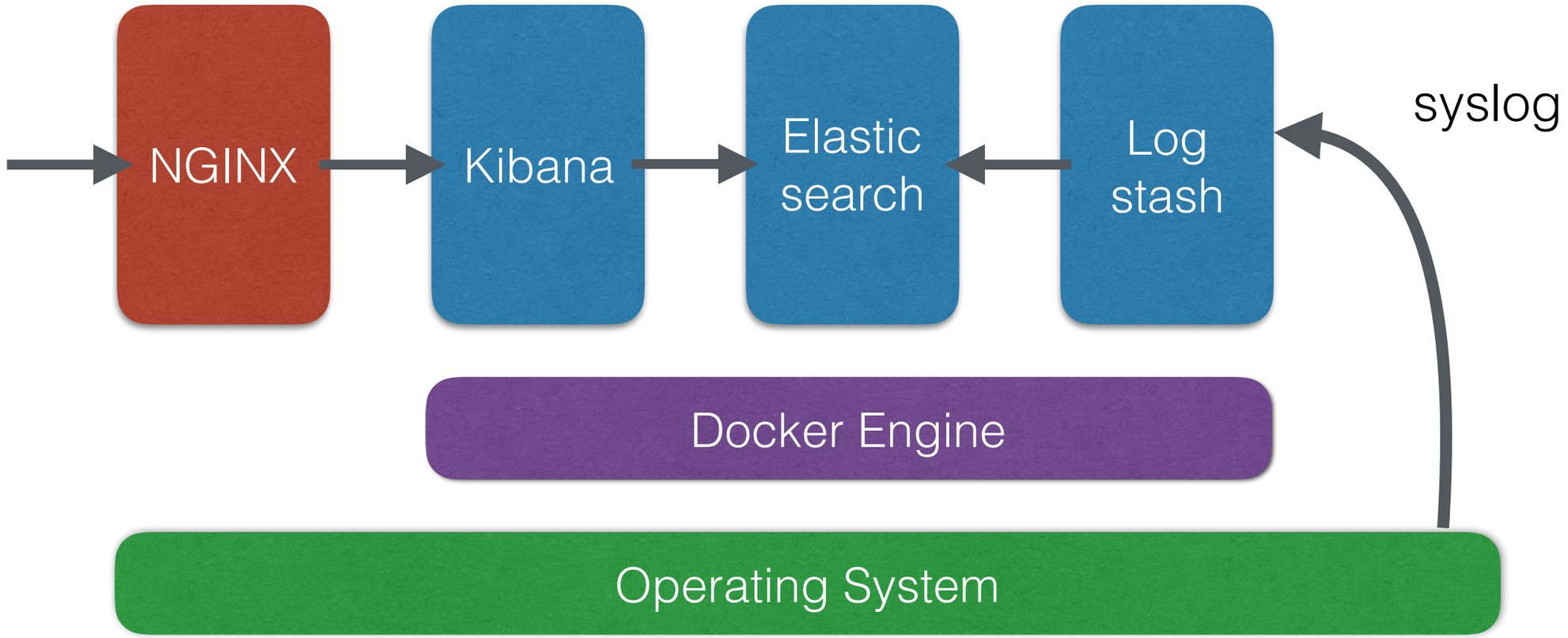
- Use official Docker packages, configure

  https://hub.docker.com/

ELK Phoenix Server

- Grab Ubuntu 14.04 box from digitalocean.com
- Install Firewall & Frontend NGINX Proxy
- Install Docker
- Install ELK on Docker from official repository
- Feed syslog to ELK

ELK Phoenix Server



Demo

Q & A

https://github.com/woditschka
bernhard@woditschka.com
Twitter: @woditschka

https://www.elastic.co
https://www.docker.com
https://hub.docker.com
https://cloud.digitalocean.com