Making Sense of Logs

Example of using the ELK Stack

Martin Petrovsky
Tech Architect / CQ5 Specialist

Who am I?

+5 years involved in sling (ok it was CQ5)
14+ years as Java dev and later tech architect
Current interests:

- docker
- scalable & resilient architectures
- running effective teams
- http://uk.linkedin.com/in/martinpetrovsky

So what's the problem?

- When logs are not **consolidated** and **searchable** they loose their value
- When logs are not monitored for critical errors then you running your business **blind**
- If you not monitoring your key business processes/metrics then it may be too late to realise you have a problem

Solutions

- There are many open source & propriety solutions
- ELK – Elasticsearch + Logstash + Kibana

Nagios®

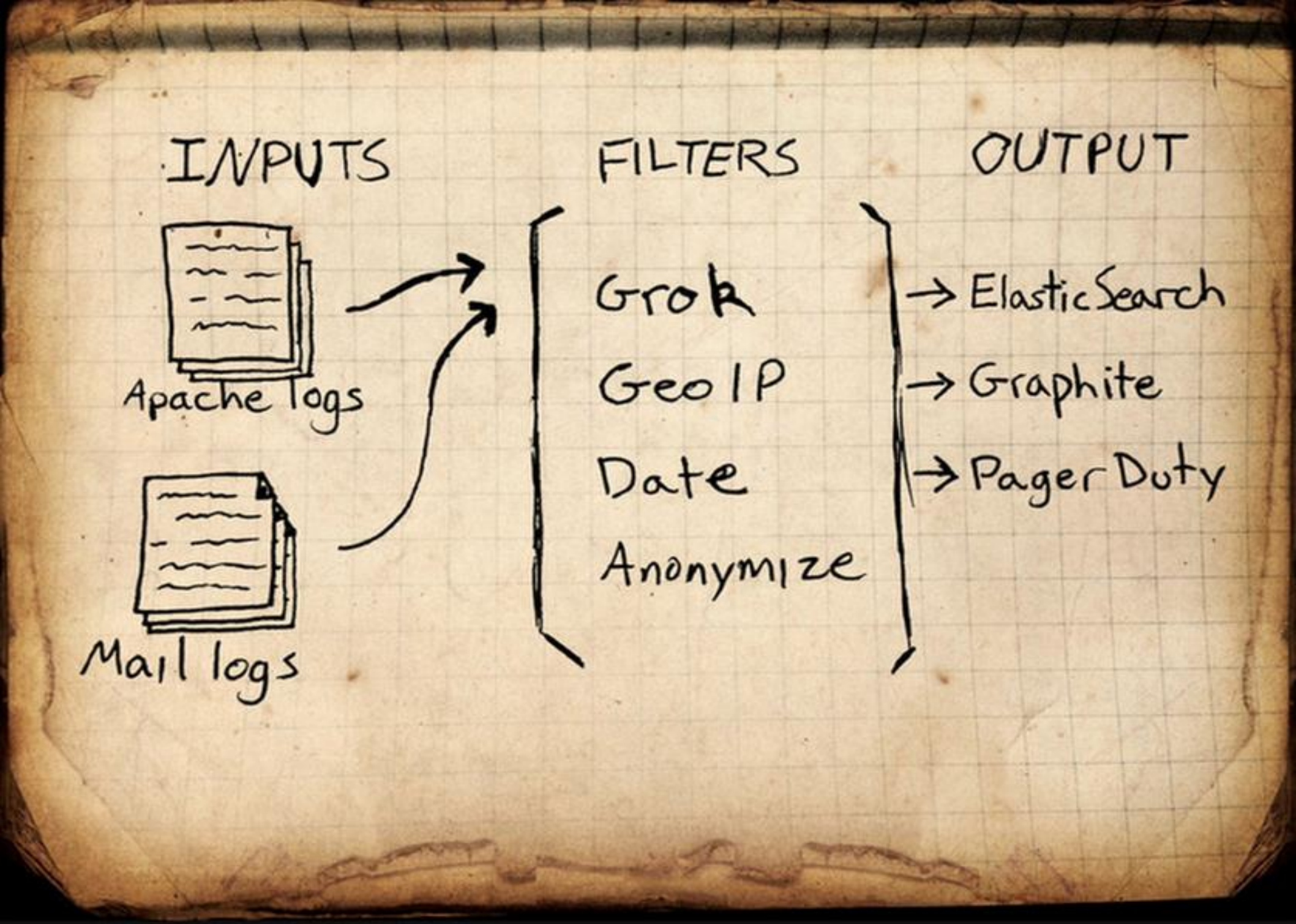
Ganglia

ZABBIX

graphite

Today

- Using Logstash + Elastic Search/Kibana for monitoring logs
- How to set it up
- Demo of a real life outage



Source: https://speakerdeck.com/monitorama/boston-2013-session-jordan-sissel

Example

- Sling error logs
- Sling request logs
- GC logs
- Dispatcher Logs
- Apache Logs

Questions?

- Samples will be uploaded to https://github.com/marto
- Checkout the usual resources:
  - logstash.net
  - http://www.elasticsearch.org/overview/kibana/
  - ELK stack - http://www.elasticsearch.org/overview/elkdownloads