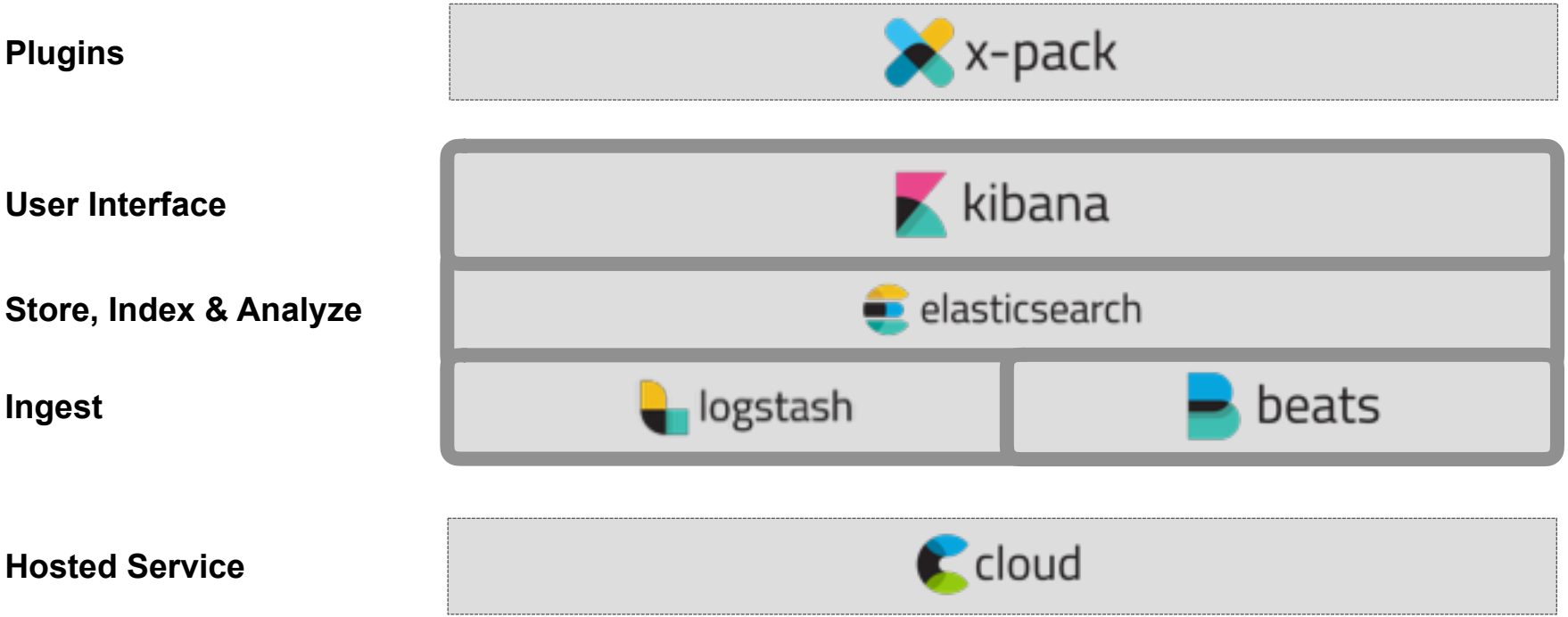
elastic

David Pilato
Developer | Evangelist
@dadoonet

And the beats go on!

The Elastic Stack



elastic

beats

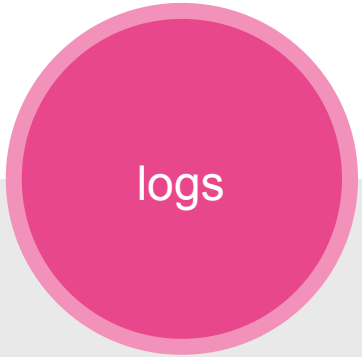
Beats are lightweight shippers that collect and ship all kinds of operational data to Elasticsearch

elastic

Examples of operational data

Packetbeat

Topbeat

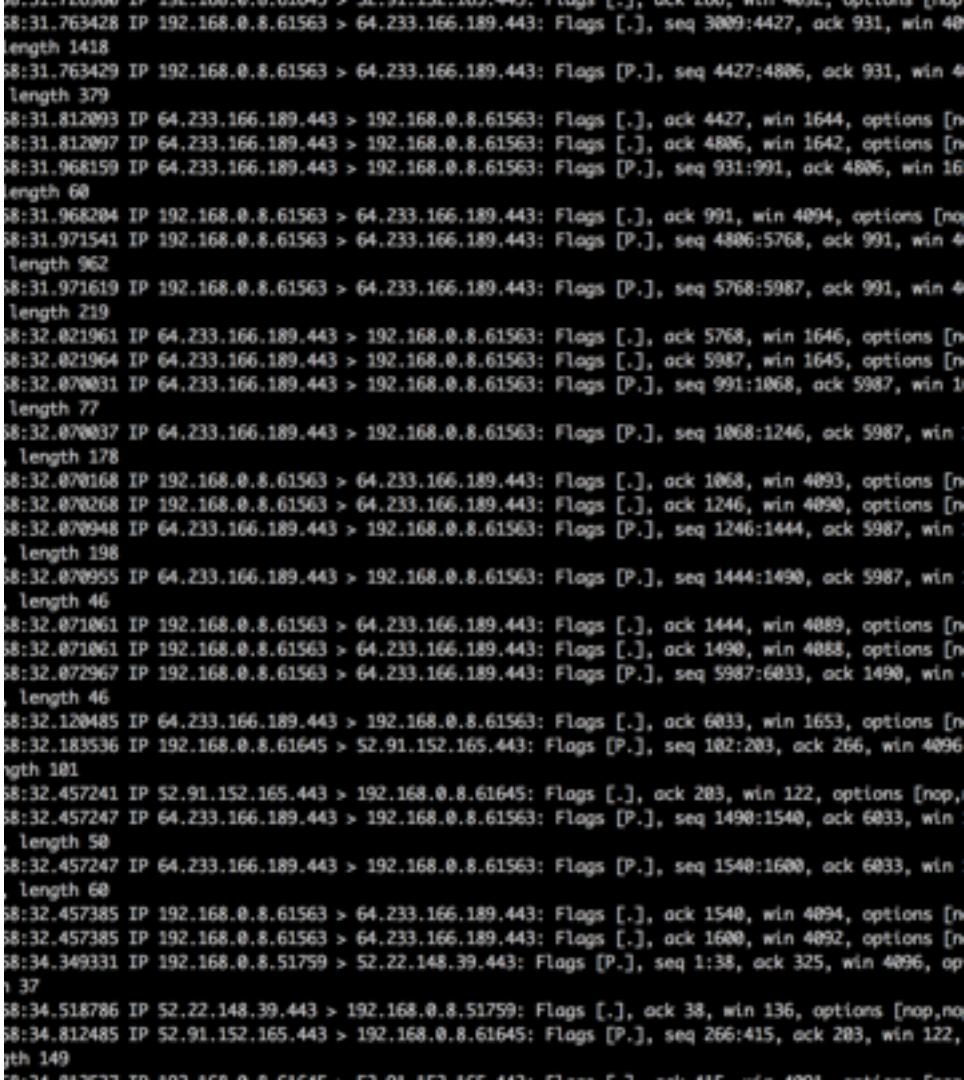


Filebeat
Winlogbeat

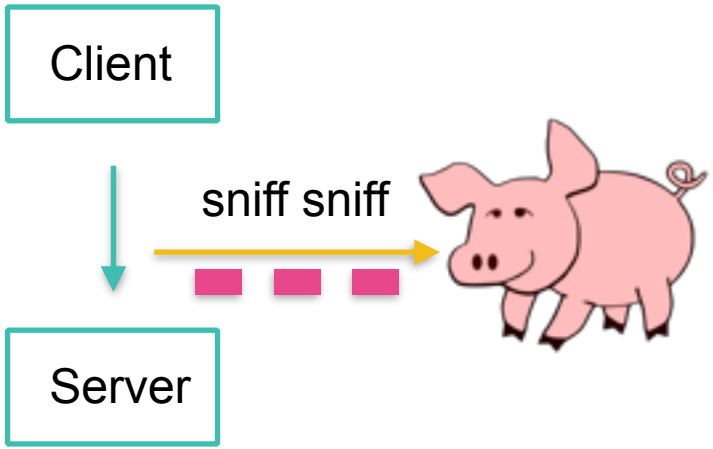
elastic

Packetbeat

Captures insights from network packets



Sniffing the network traffic



- Copy traffic at OS or hardware level
- Is completely passive
- ZERO latency overhead
- Not in the request/response path, cannot break your application

elastic

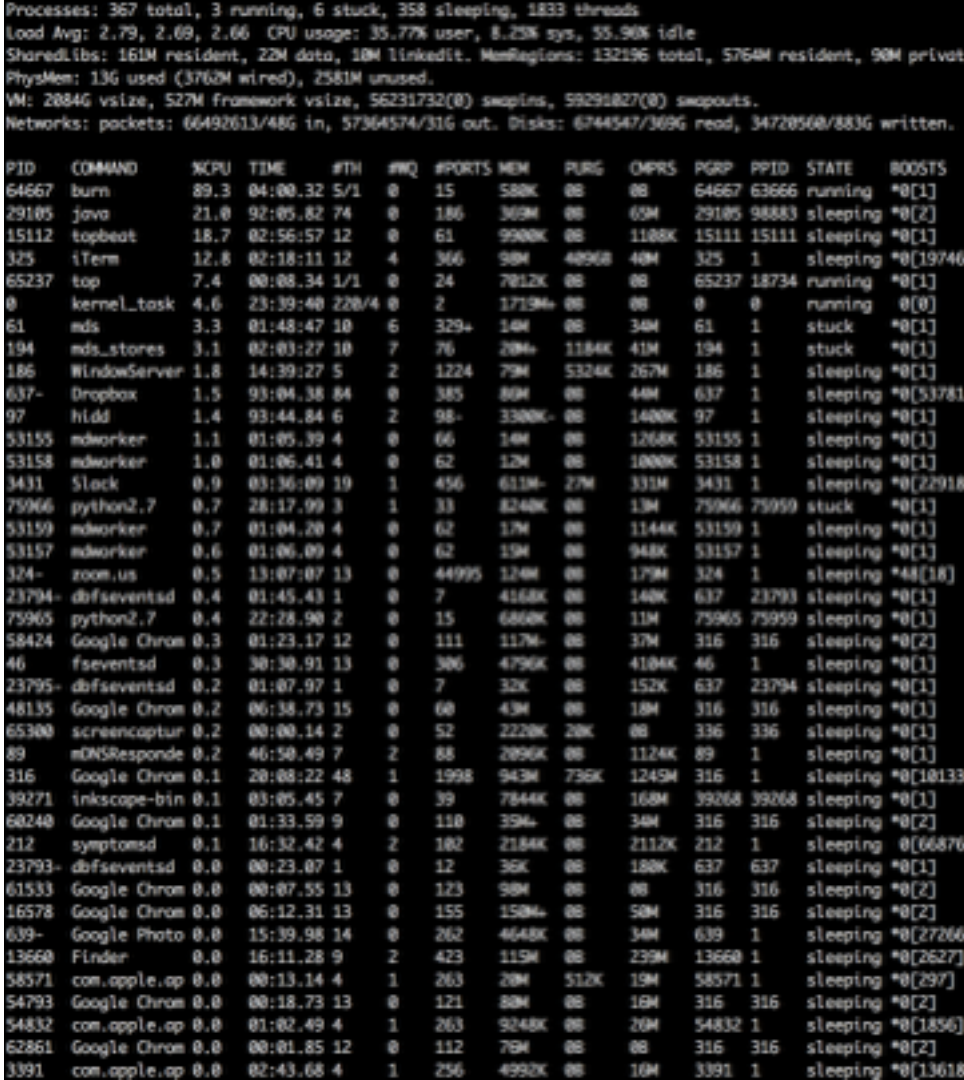
Packetbeat: Available decoders

- HTTP
- MySQL
- PostgreSQL
- Redis
- Thrift-RPC
- Memcache
- MongoDB
- ICMP
- DNS
- AMQP
- + Add your own

elastic

Topbeat

Like the Unix **top** command but sends the output periodically to Elasticsearch. Also works on Windows.



Topbeat: Exported data

System wide

- system load
- total CPU usage
- CPU usage per core
- Swap, memory usage

Per process

- state
- name
- command line
- pid
- CPU usage
- memory usage

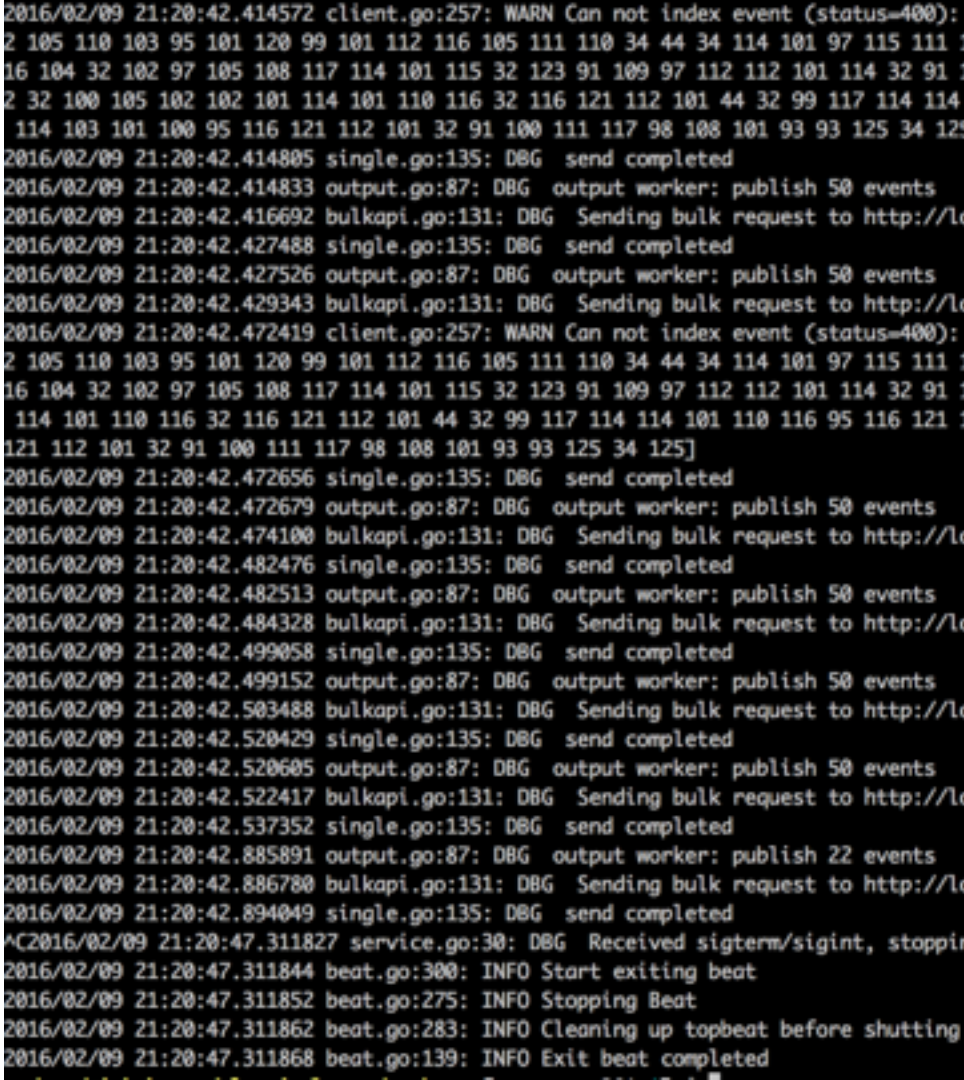
Disk usage

- available disks
- used, free space
- mounted points

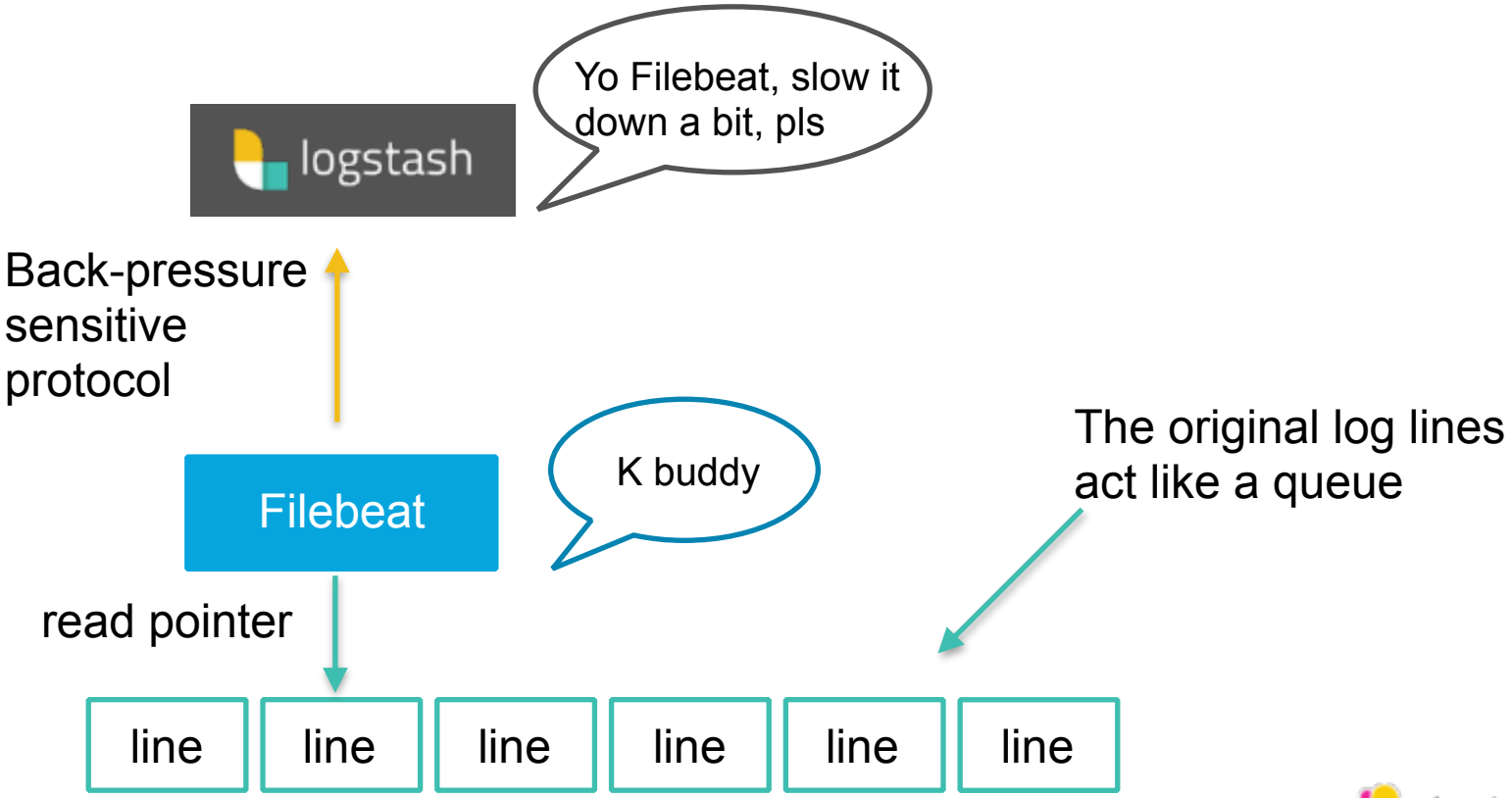
elastic

Filebeat

Forwards log lines to Elasticsearch



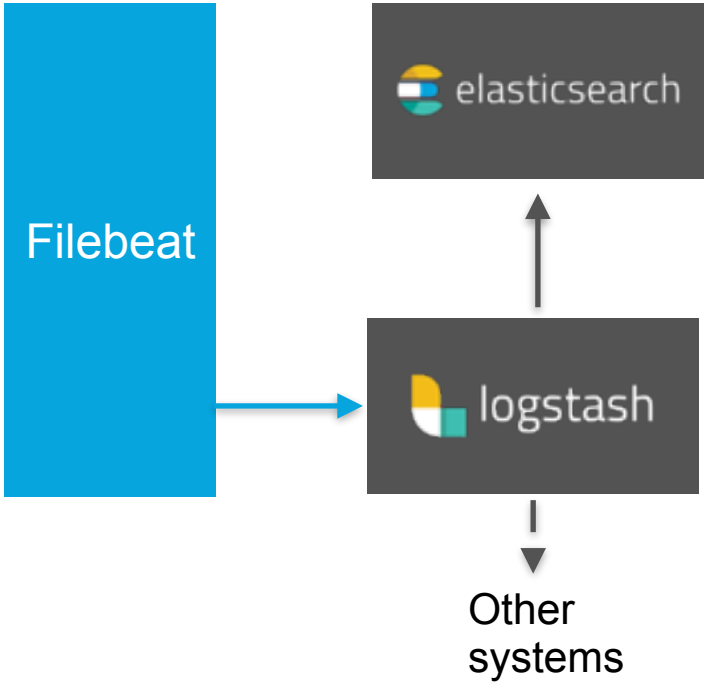
Filebeat: Never lose a log line



elastic

Filebeat: Parse logs with Logstash

Parse logs with Logstash

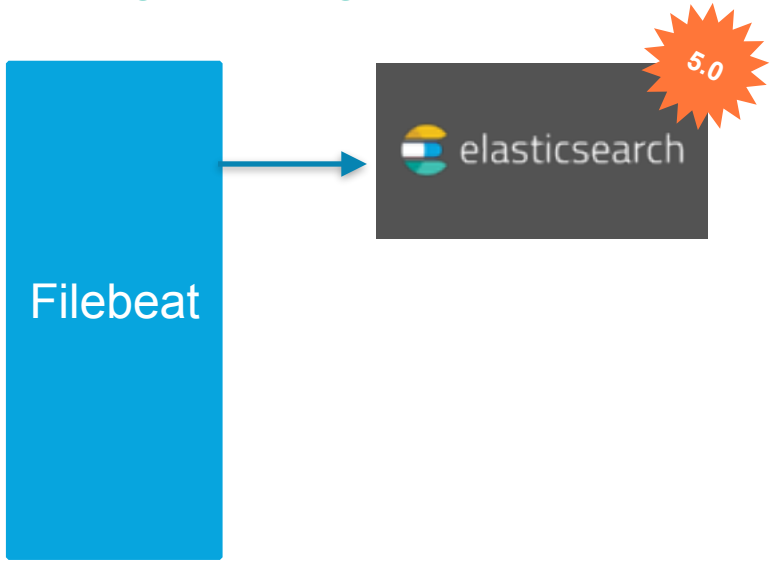


- Filebeat sends out unparsed log lines
- Use filters from Logstash to parse the log lines
- Flexible, with conditionals & custom filters
- Forward data to other systems using the Logstash output plugins

elastic

Filebeat: Parse logs with Ingest Node

Parse logs with Ingest node in Elasticsearch

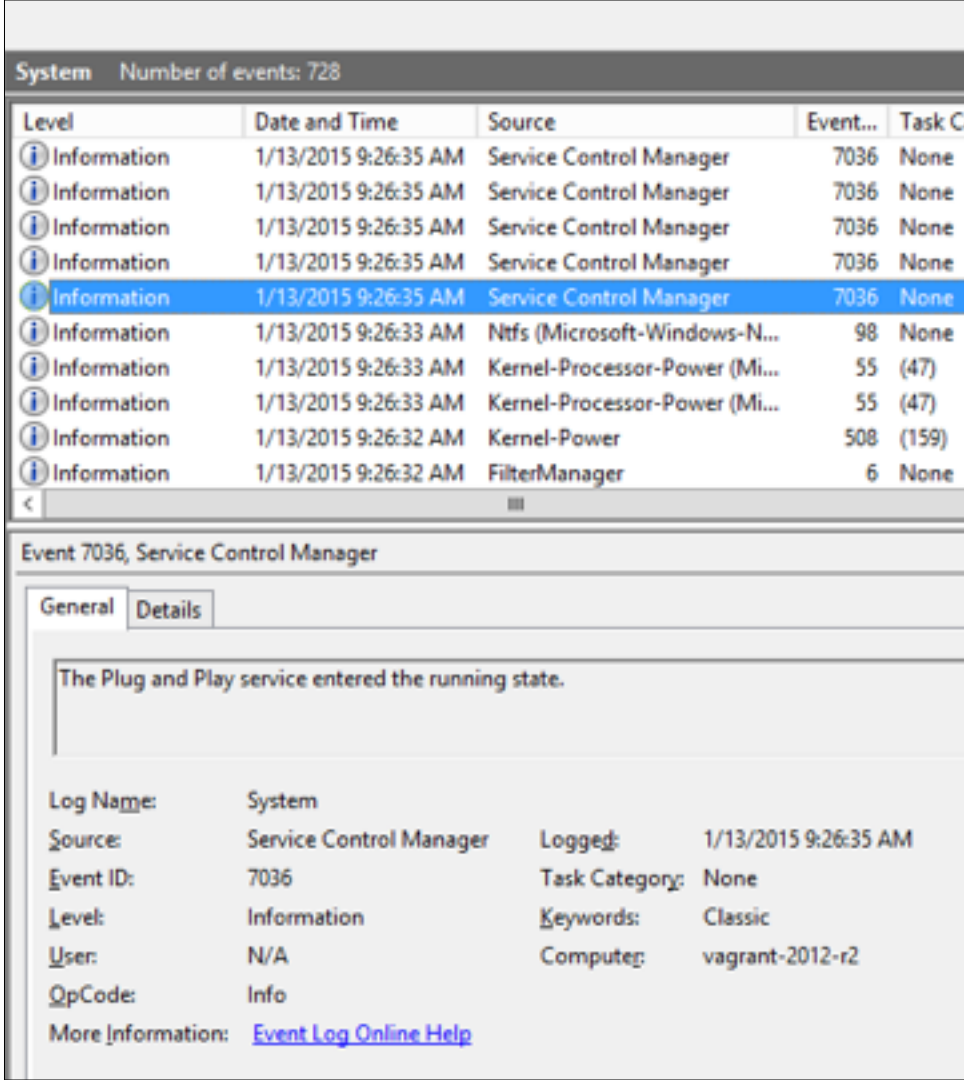


- Filebeat sends out unparsed log lines directly to Elasticsearch
- Use Ingest Node processors (grok, geoip…) to parse the log lines
- Easier to setup

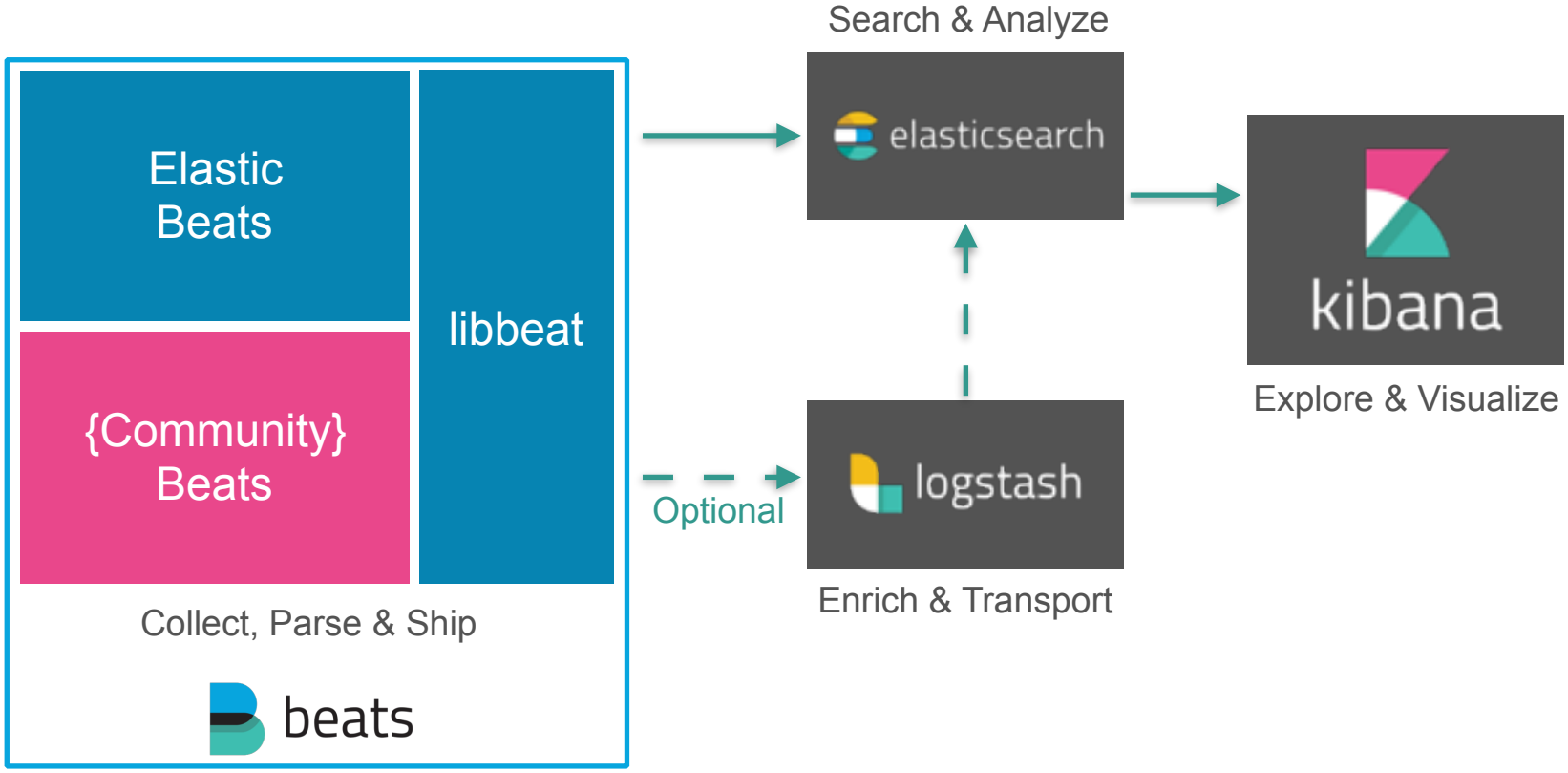
elastic

Winlogbeat

Forwards Windows Event logs to Elasticsearch

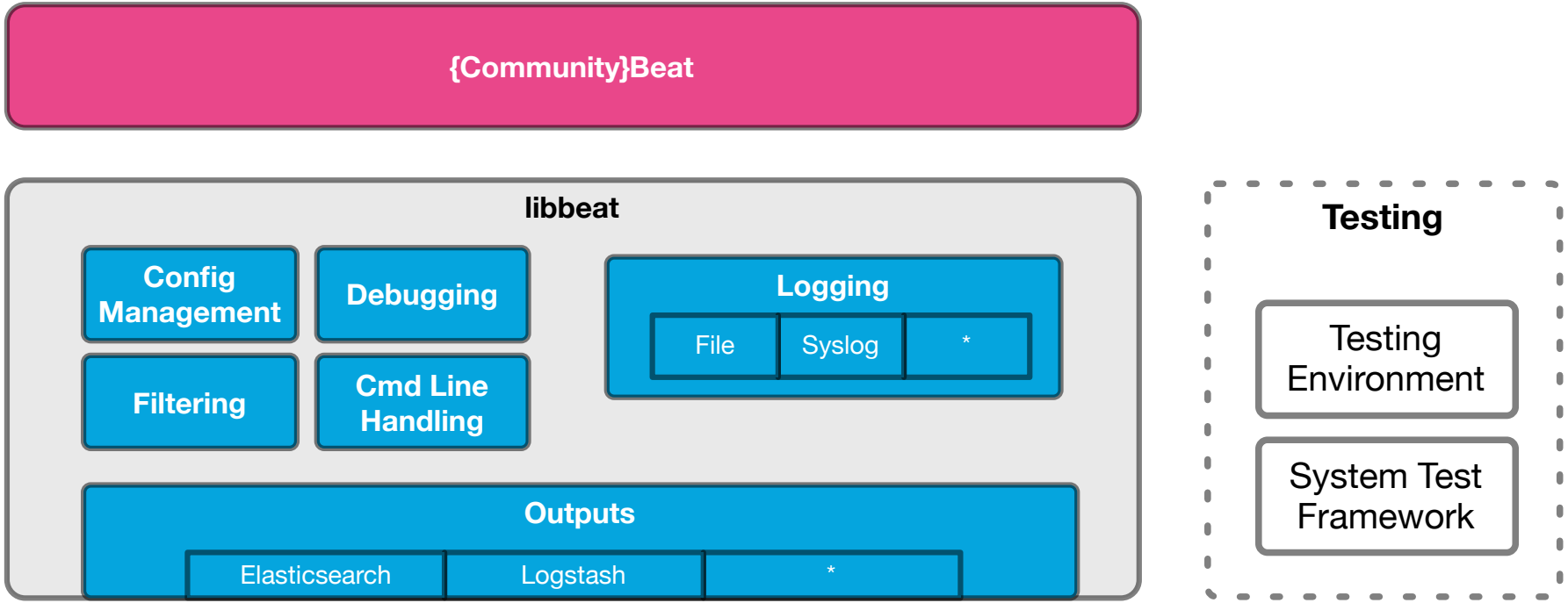


Beats Platform



elastic

Architecture Overview - libbeat



elastic

Beats Packer

Produces RPMs, DEBs, …

https://github.com/elastic/beats-packer


Super-Sound-Single
45 rpm
Disco-Remix
THE WHISPERS
RCA
And The Beat Goes On
7:30
Side 1
Can You Do The Boogie
6:07
Side 2
FC 1895
Top Hit
USA

elastic

topbeat, packetbeat and soundbeat

https://github.com/dadoonet/soundbeat

thanks!

https://github.com/dadoonet/soundbeat