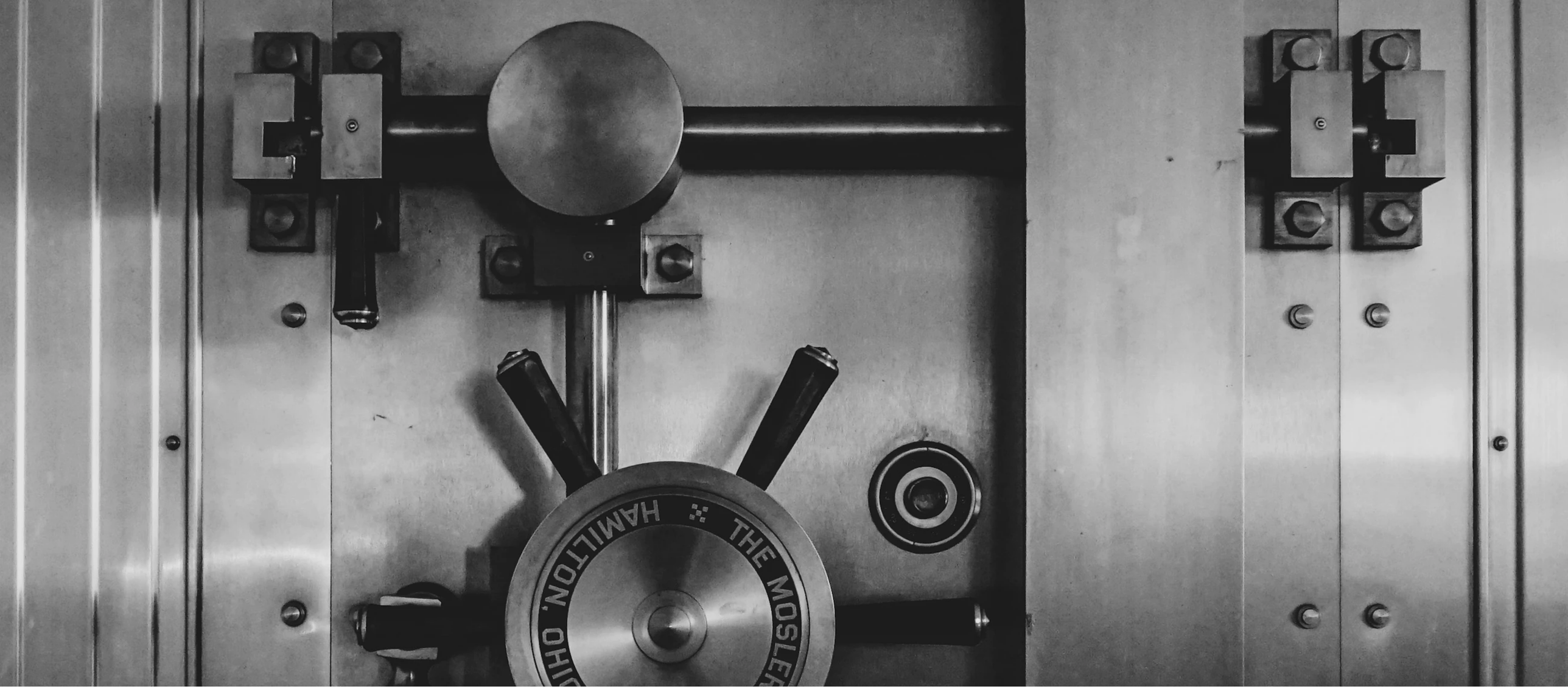


Storing and Processing data

Kresten Jacobsen

What is a SIEM?

Capabilities of a SIEM

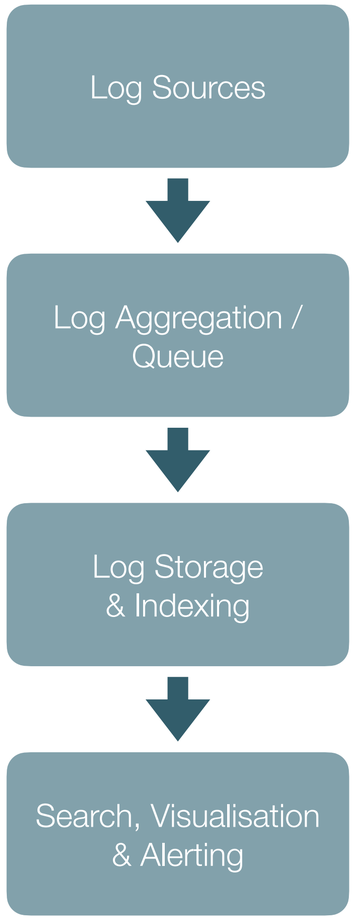
- Log Aggregation
- Searching
- Correlation
- Alerting
- Dashboarding (visualisation)
- Retention (log storage)
- Forensics Analysis

What is a SIEM?

Capabilities of a SIEM

- Log Aggregation
- Searching
- Correlation
- Alerting
- Dashboarding (visualisation)
- Retention (log storage)
- Forensics Analysis

Example Architecture of a SIEM

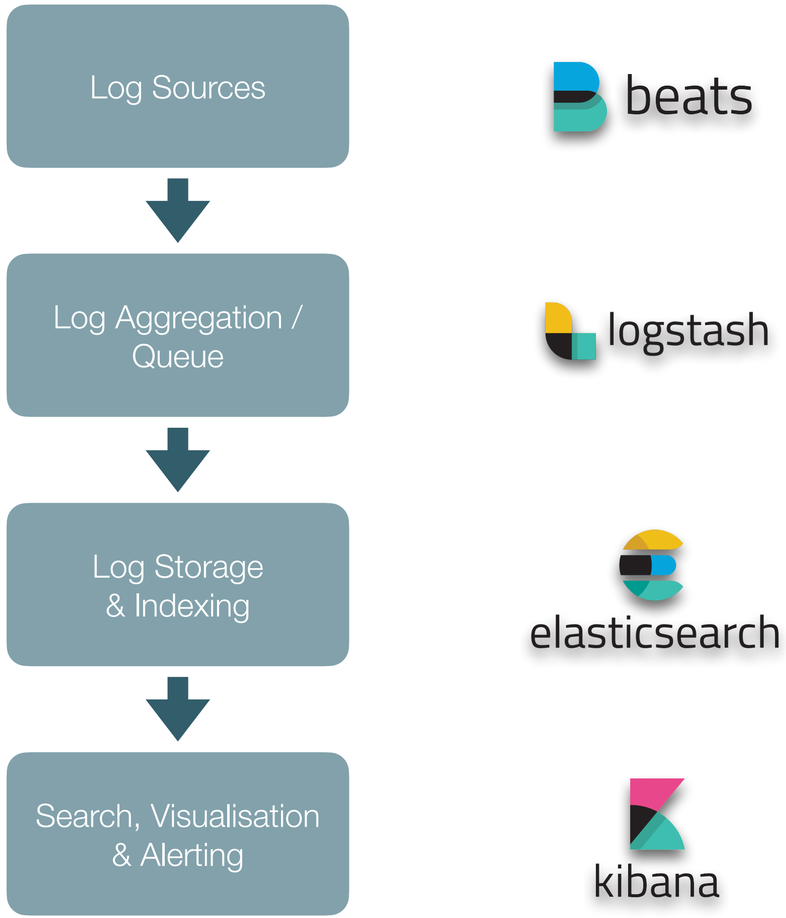


What is a SIEM?

Capabilities of a SIEM

- Log Aggregation
- Searching
- Correlation
- Alerting
- Dashboarding (visualisation)
- Retention (log storage)
- Forensics Analysis

Example Architecture of a SIEM

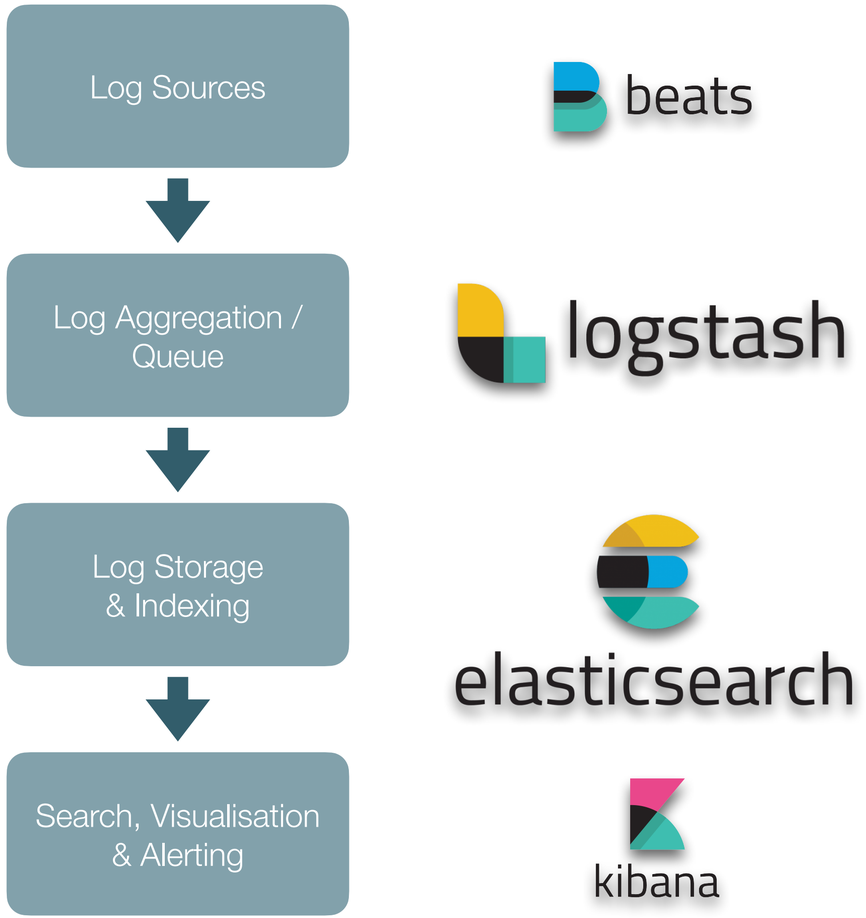


What is a SIEM?

Capabilities of a SIEM

- **Log Aggregation**
- Searching
- Correlation
- Alerting
- Dashboarding (visualisation)
- **Retention (log storage)**
- Forensics Analysis

Example Architecture of a SIEM



Data Sources

Network

- Full Packet Capture
- Netflow

Servers

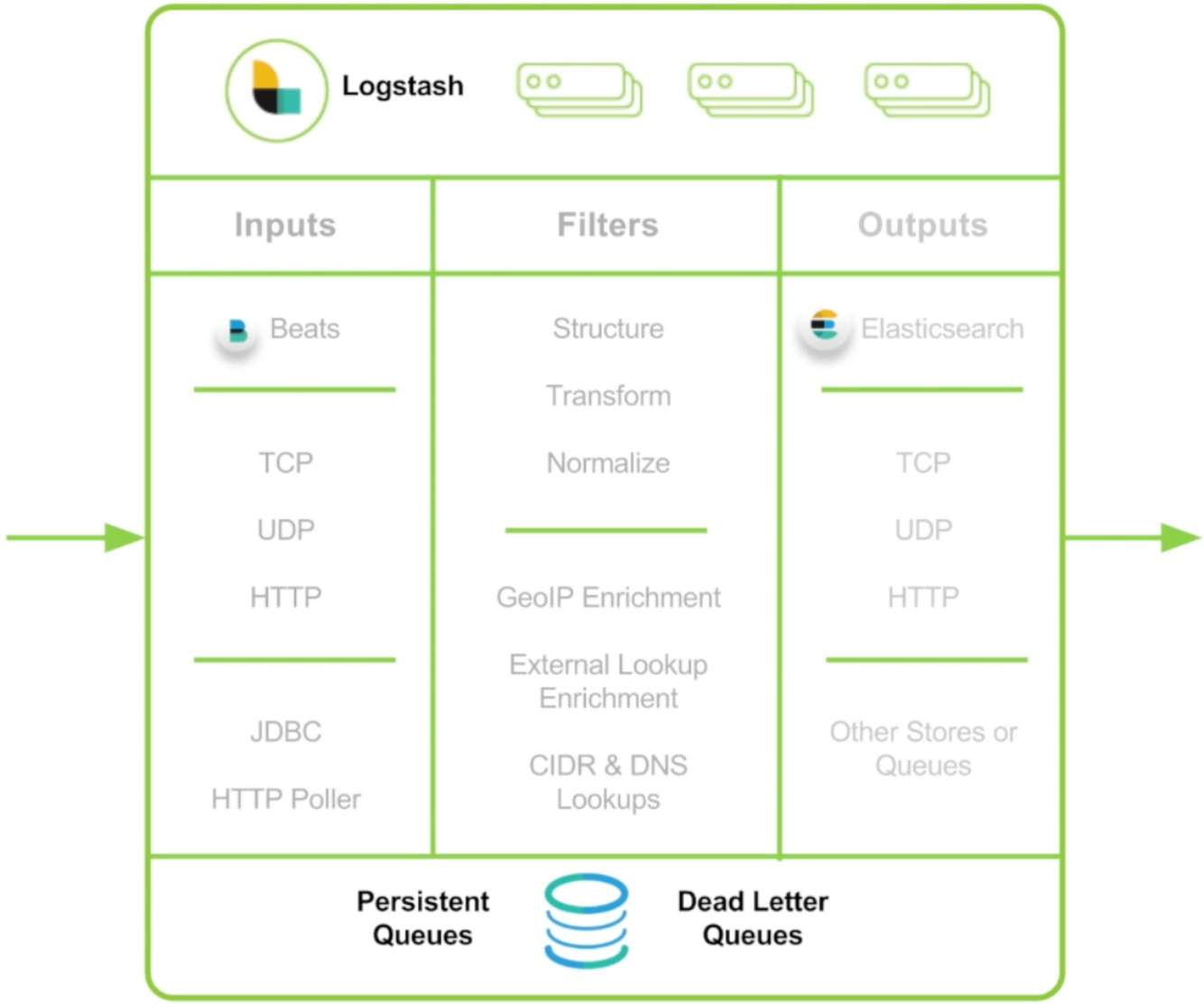
- OS logs
  - Syslog
  - EventLogs (or better Sysmon)
- Application logs (esp. compliance)

Hosts

- OS logs

GROK ALL THE THINGS!

Logstash architecture



Logstash architecture (cont'd)

```
~/D/filebeat-6.0.1-darwin-x86_64 $ cat sample.log
2007-03-01T13:00:00Z I met a traveller from an antique land
2007-03-01T14:00:00Z Who said—“Two vast and trunkless legs of stone
2007-03-01T15:00:00Z Stand in the d
2007-03-01T16:00:00Z Half sunk a sh
2007-03-01T17:00:00Z And wrinkled l
2007-03-01T18:00:00Z Tell that its
2007-03-01T19:00:00Z Which yet surv
2007-03-01T20:00:00Z The hand that
2007-03-01T21:00:00Z And on the ped
2007-03-01T22:00:00Z My name is Ozy
2007-03-01T23:00:00Z Look on my Wor
2007-04-01T00:00:00Z Nothing beside
2007-04-01T01:00:00Z Of that coloss
2007-04-01T02:00:00Z The lone and l
~/D/filebeat-6.0.1-darwin-x86_64 $
```

```
~/D/logstash-6.0.1 $ cat sample.conf
input {
  beats { port => 5044 }
}

filter {
  grok {
    match => [
      "message", "%{TIMESTAMP_ISO8601:timestamp_string}%{SPACE}%{GREEDYDATA:line}"
    ]
  }

  date {
    match => ["timestamp_string", "ISO8601"]
  }

  mutate {
    remove_field => [message, timestamp_string]
  }
}

output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    user => elastic
    password => "cio64ax5-m2&0QU*hR#&"
  }

  stdout {
    codec => rubydebug
  }
}
~/D/logstash-6.0.1 $
```

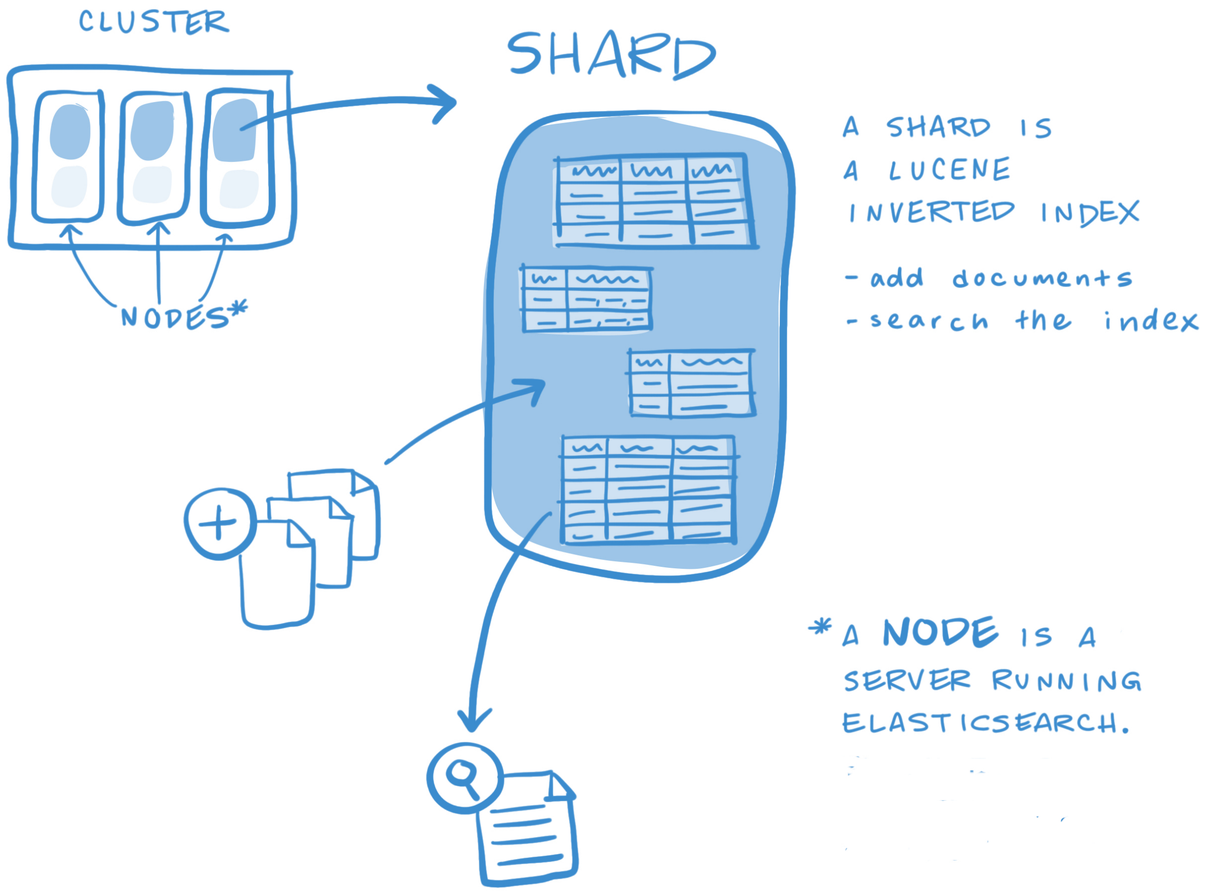
```
{
    "@timestamp" => 2007-04-01T01:00:00.000Z,
        "offset" => 875,
          "line" => "Of that colossal Wreck, boundless and bare ",
      "@version" => "1",
          "beat" => {
            "name" => "avce",
        "hostname" => "avce",
         "version" => "6.0.1"
    },
          "host" => "avce",
    "prospector" => {
        "type" => "log"
    },
        "source" => "/Users/andrewcholakian/Downloads/filebeat-6.0.1-darwin-x86_64/sample.log",
          "tags" => [
        [0] "beats_input_codec_plain_applied"
    ]
}
```

Source: elastic.co

Elasticsearch - storage

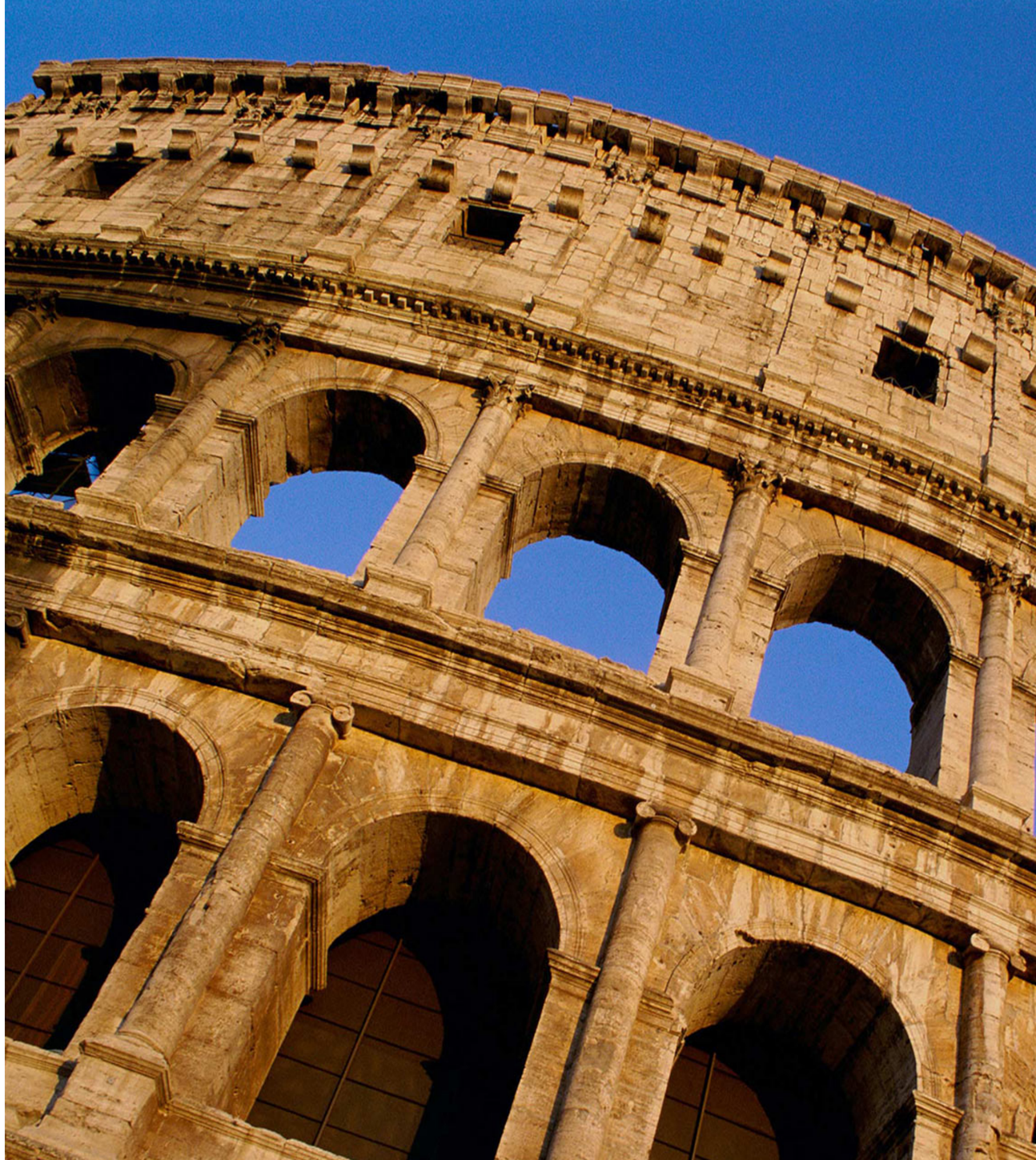
[INDSÆT BILLEDE AF ELASTICSEARCs "data" KATAALOG]

arkitekturtegning af en cluster-setup



Elasticsearch

[INDSÆT BILLEDE AF ELASTICSEARCs "data" KATAALOG]



Subject overview