Overview of SIEM

Kresten Jacobsen

What is a SIEM?

Capabilities of a SIEM

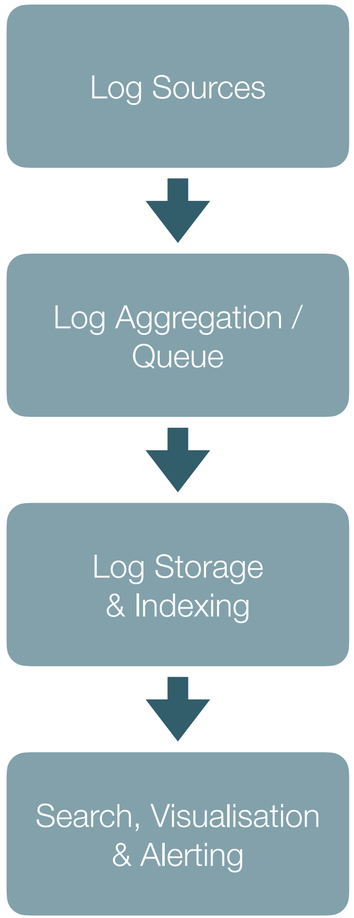
- Log Aggregation
- Searching
- Correlation
- Alerting
- Dashboarding (visualisation)
- Retention (log storage)
- Forensics Analysis

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

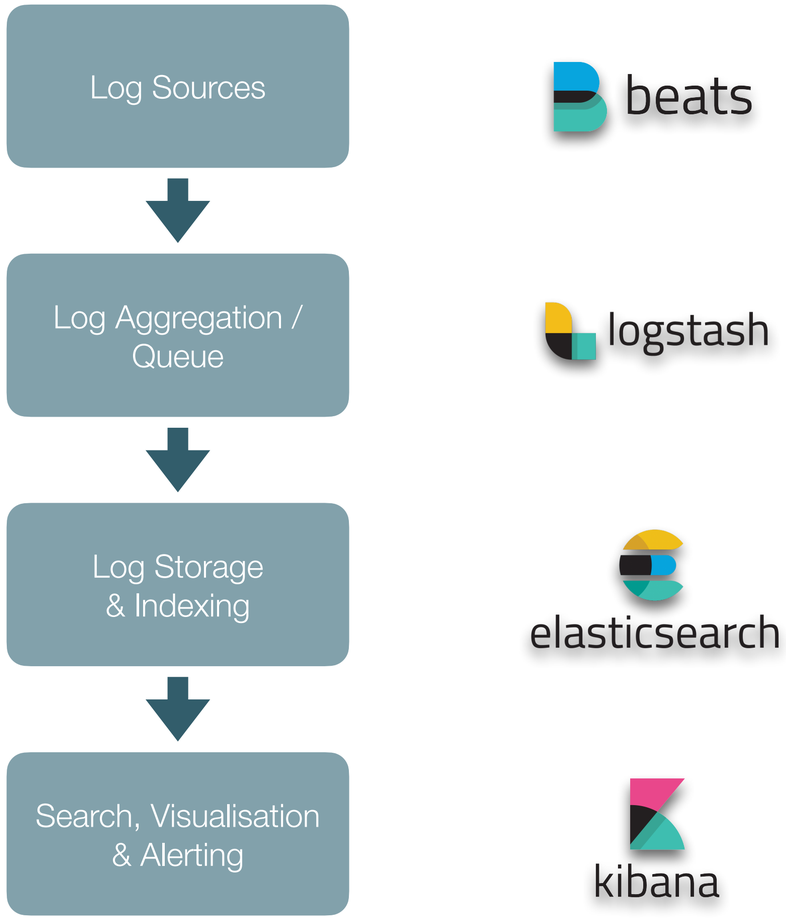


What is a SIEM?

Capabilities of a SIEM

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

Example Architecture of a SIEM

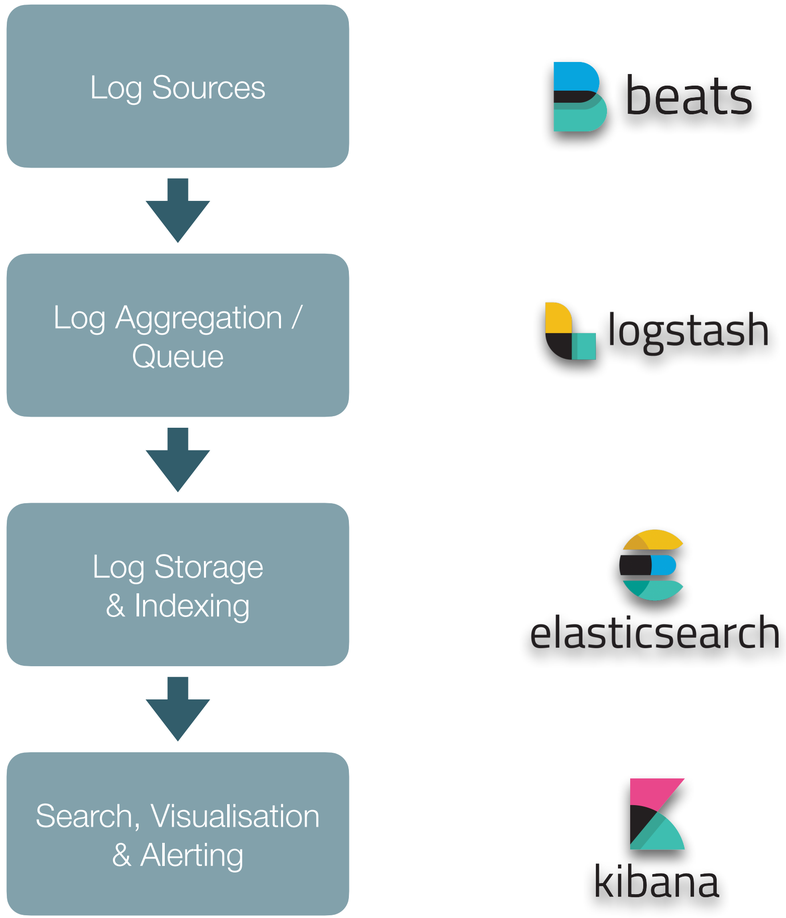


What is a SIEM?

Capabilities of a SIEM

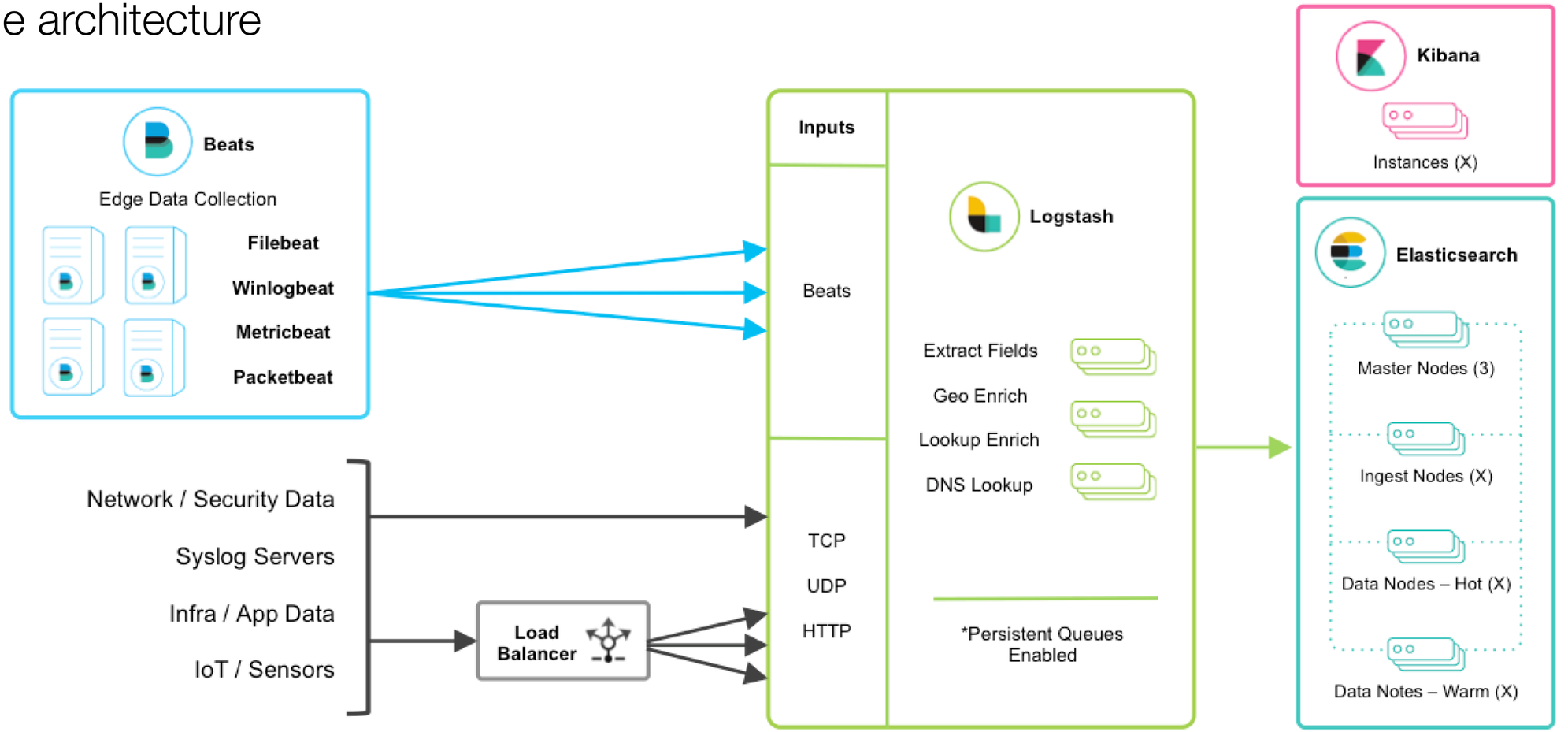
- Log Aggregation
- **Searching**
- **Correlation**
- **Alerting**
- Dashboarding (**visualisation**)
- Retention (log storage)
- Forensics Analysis

Example Architecture of a SIEM



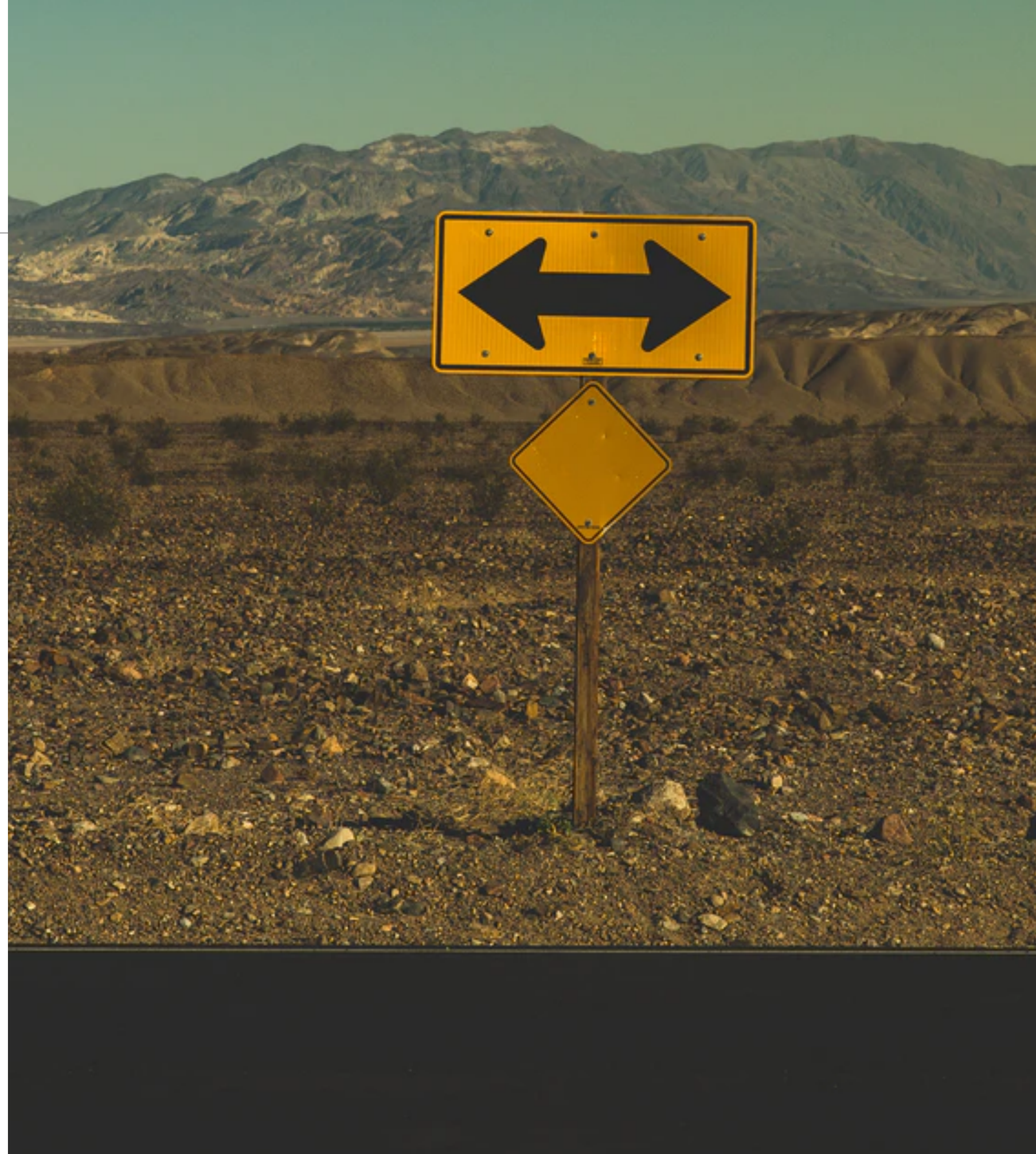
What is a SIEM?

Example architecture

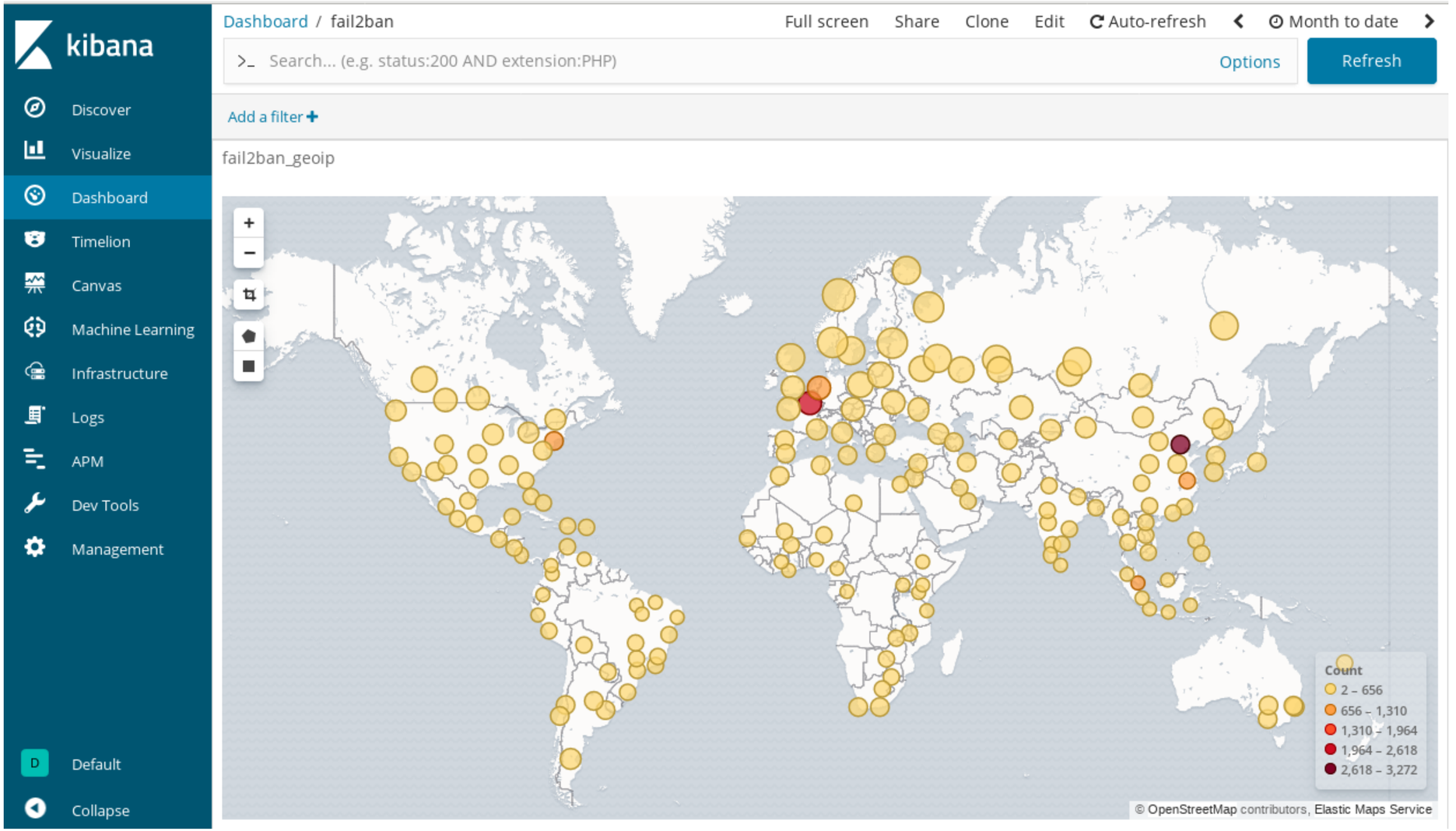


The problem with data…

- What do I search for?
- What has happened?
- Get visual!
- Get notified!

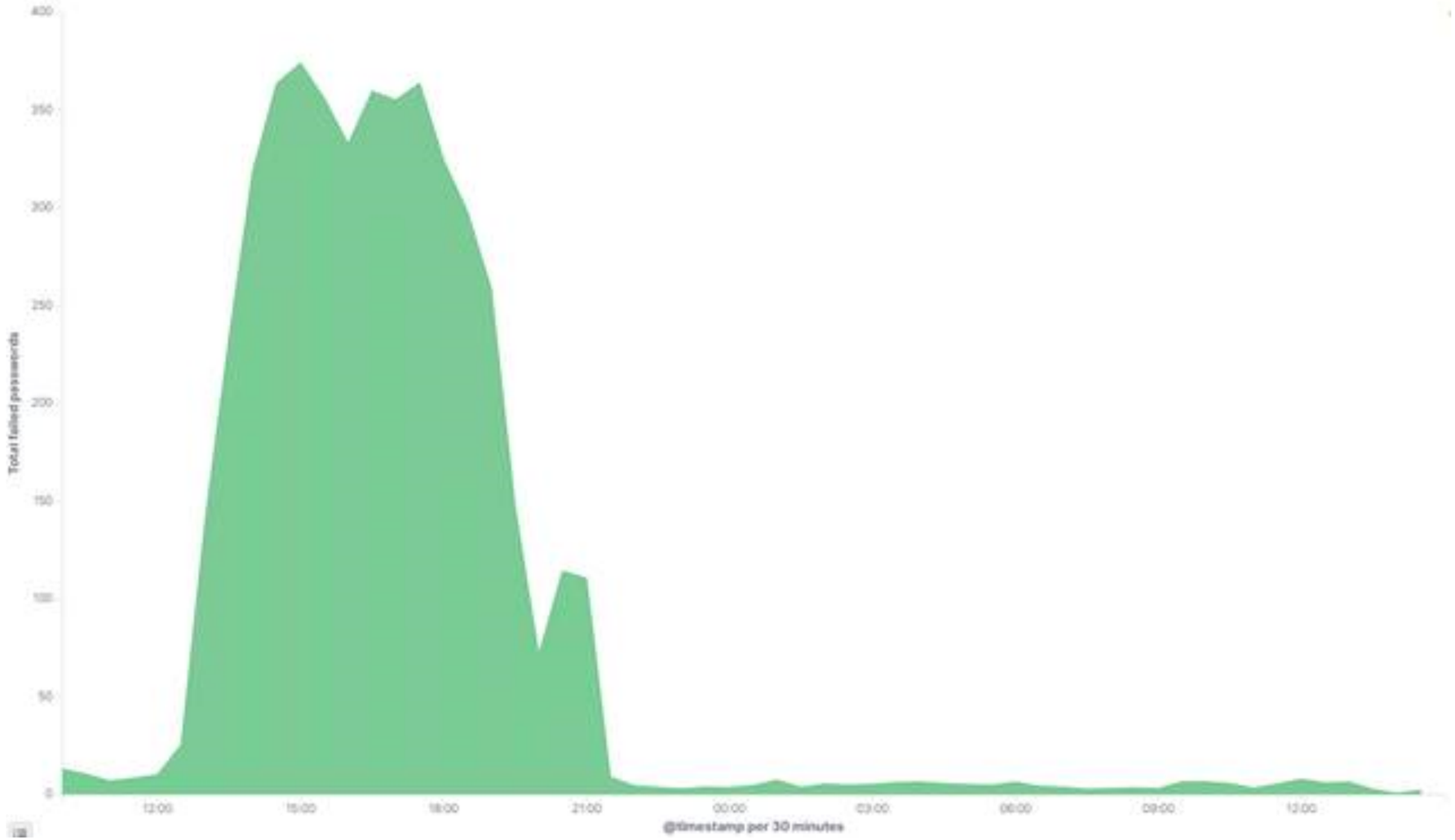


Kibana: Visualisation

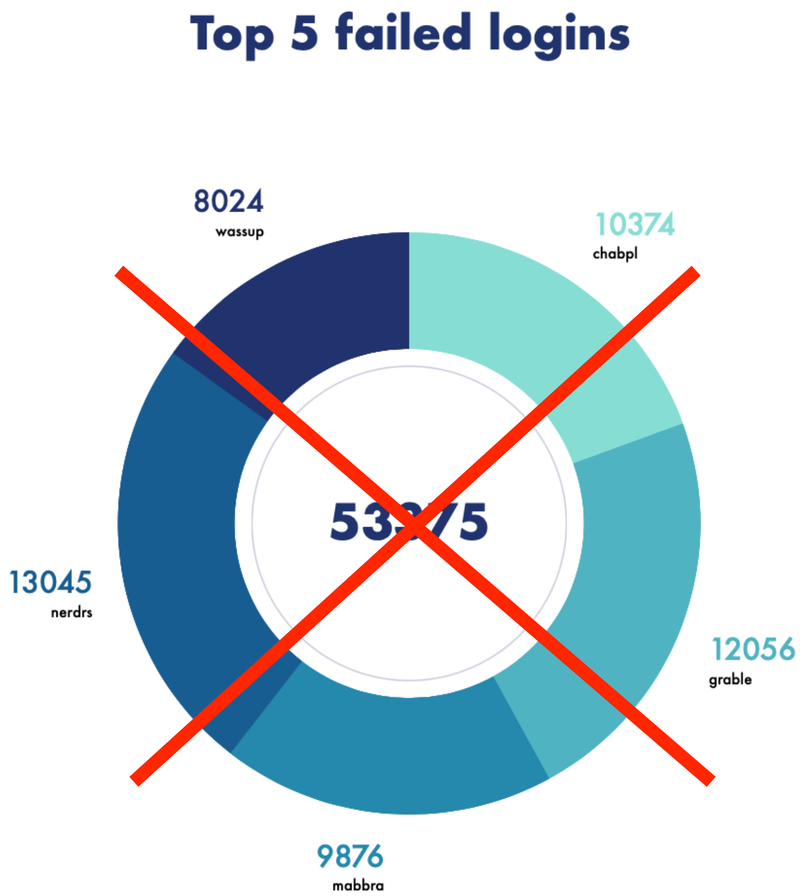


Kibana: Visualisation

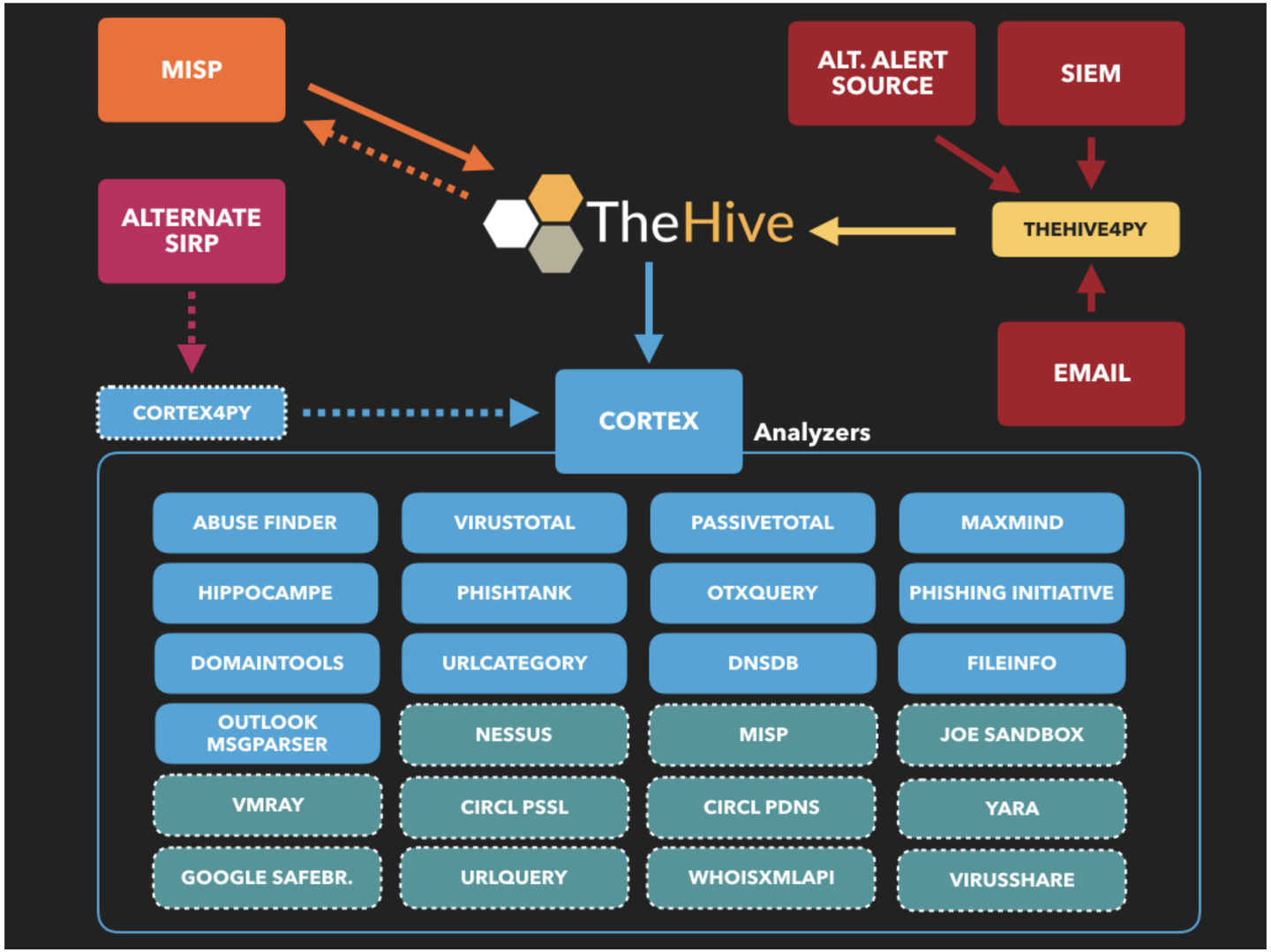
Password spray



Kibana: Visualisation (cont'd)



SOAR - Security Orchestration, Automation, and Response



Source: sans.org

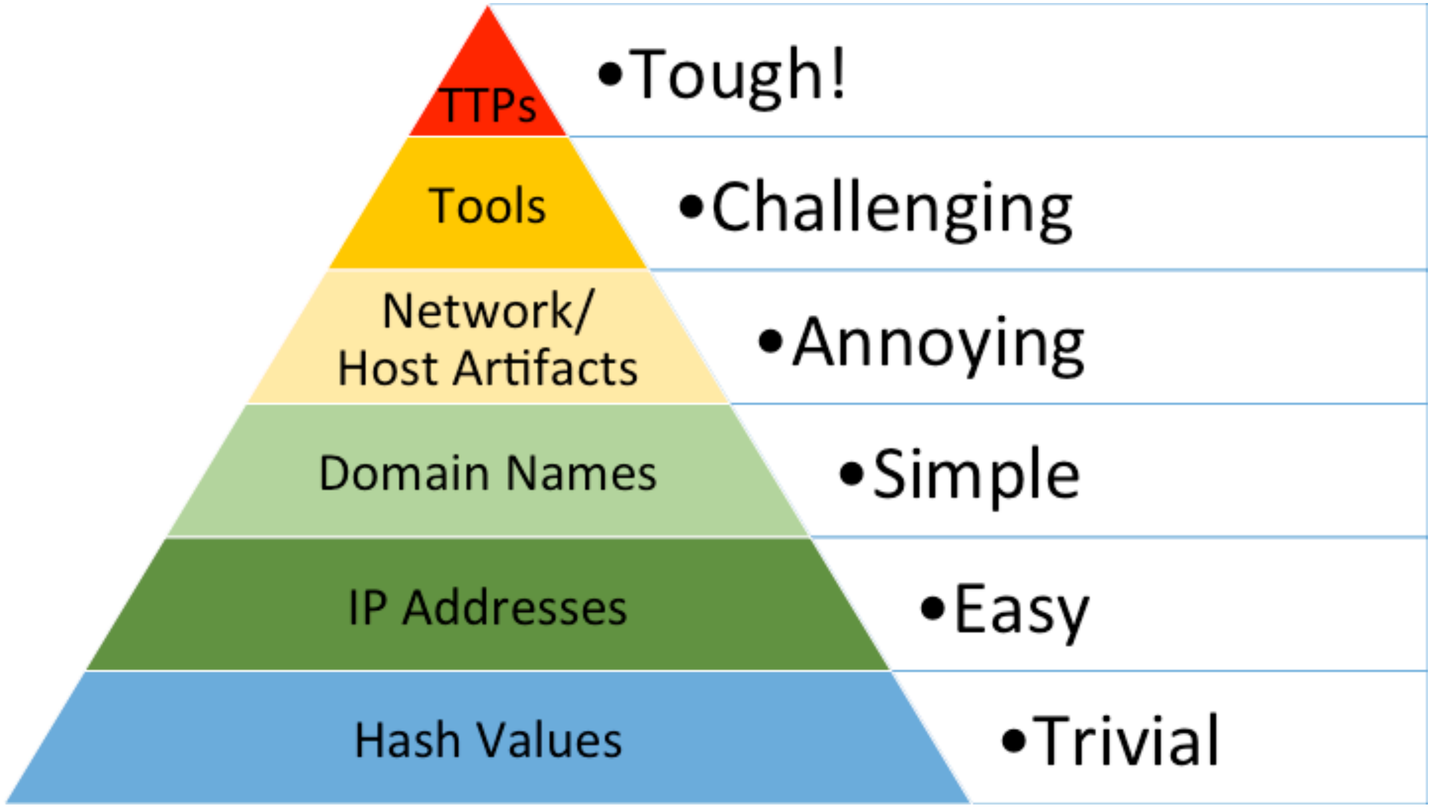
Threat feeds vs. Threat Intelligence

Threat Feeds (data enrichment)

- Known bad hashes
- Blocklists
- Known bad traffic
- Tools

Threat Intelligence (context)

- Open Source
- Closed Source



INTEGRATE! USE SOAR!

Subject overview