Overview of SIEM

Kresten Jacobsen

What is a SIEM?

Capabilities of a SIEM

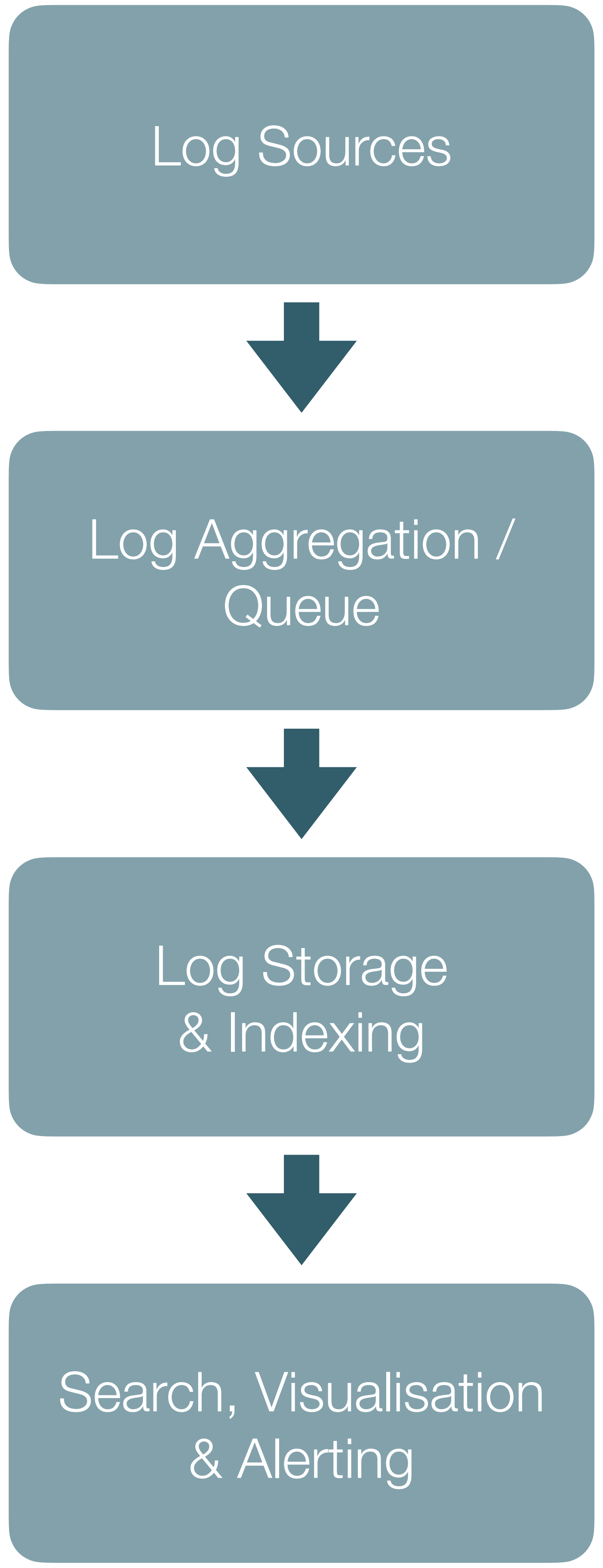
- Log Aggregation
- Searching
- Correlation
- Alerting
- Dashboarding (visualisation)
- Retention (log storage)
- Forensics Analysis

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



Log Sources

Log Aggregation / Queue

Log Storage & Indexing

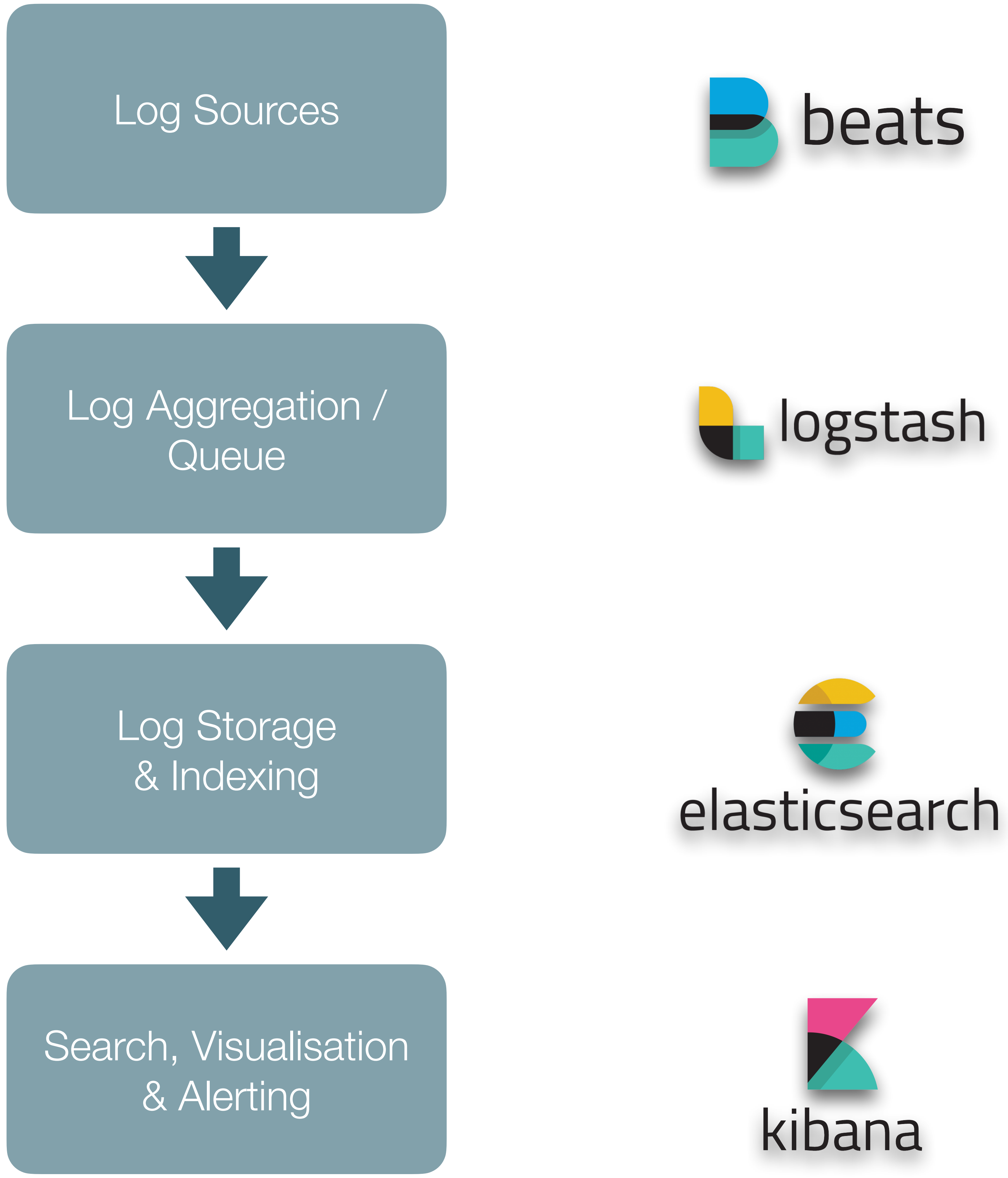
Search, Visualisation & Alerting

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



Log Sources

Log Aggregation / Queue

Log Storage & Indexing

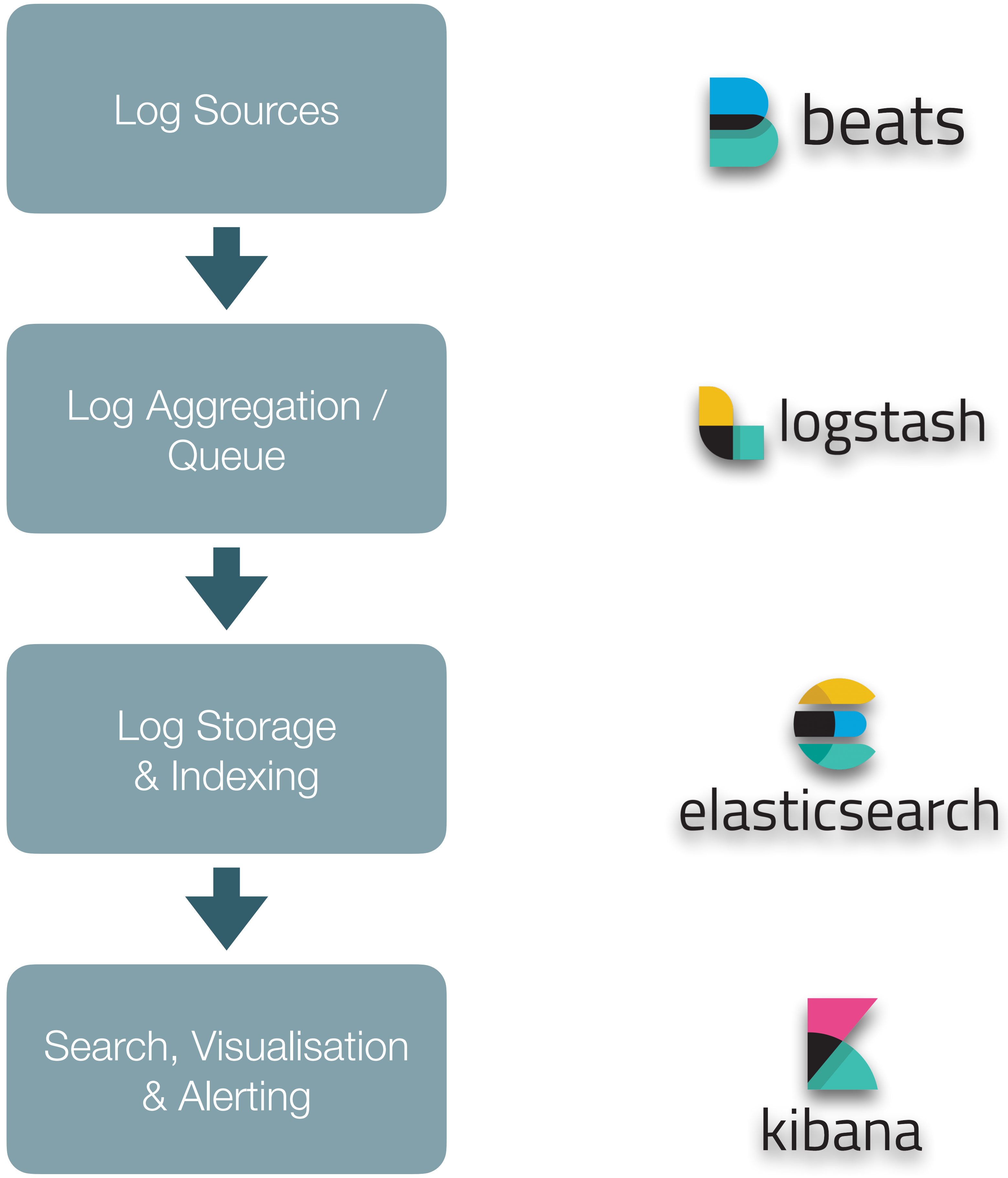
Search, Visualisation & Alerting

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



Log Sources

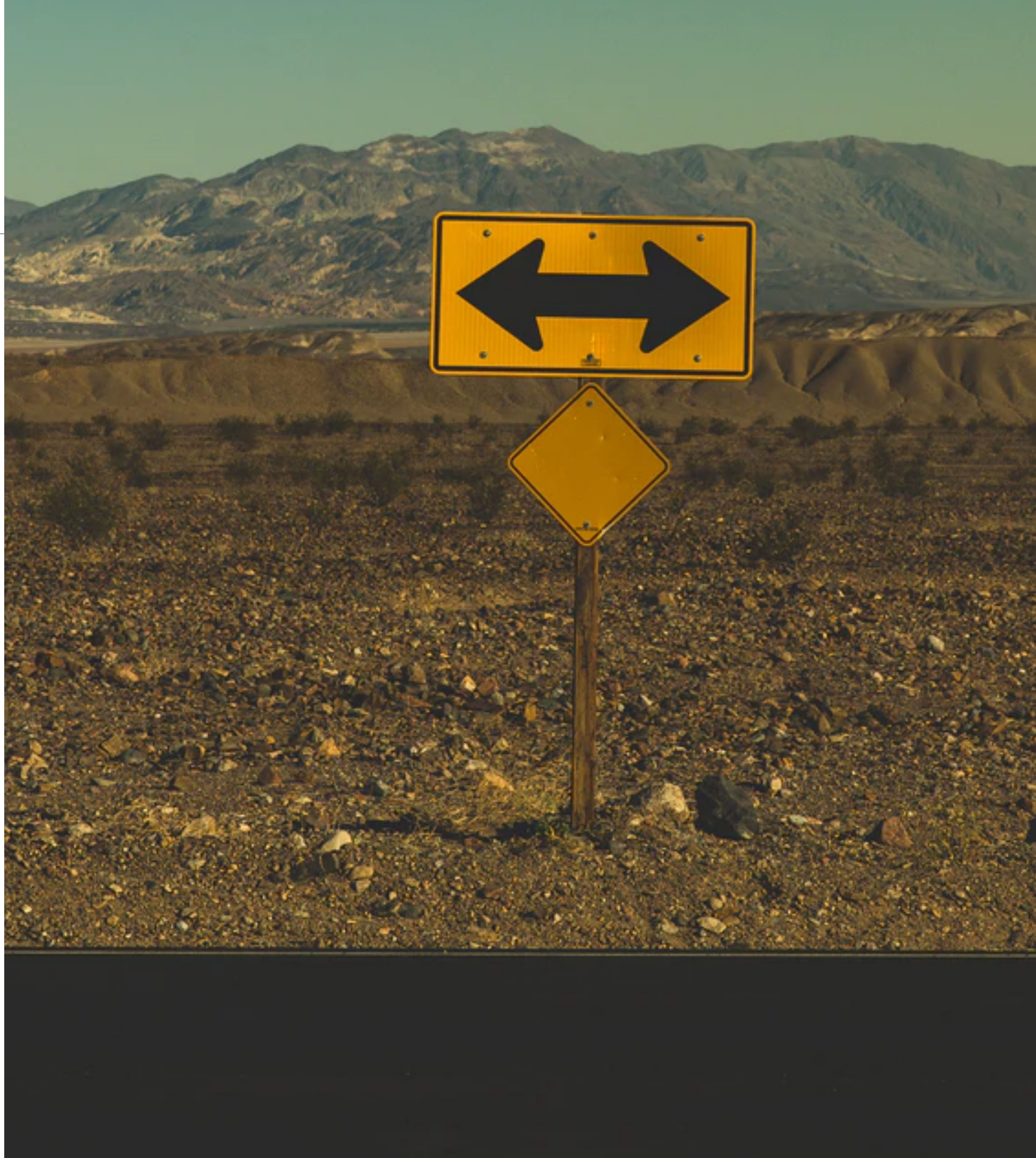
Log Aggregation / Queue

Log Storage & Indexing

Search, Visualisation & Alerting

The problem with data…

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



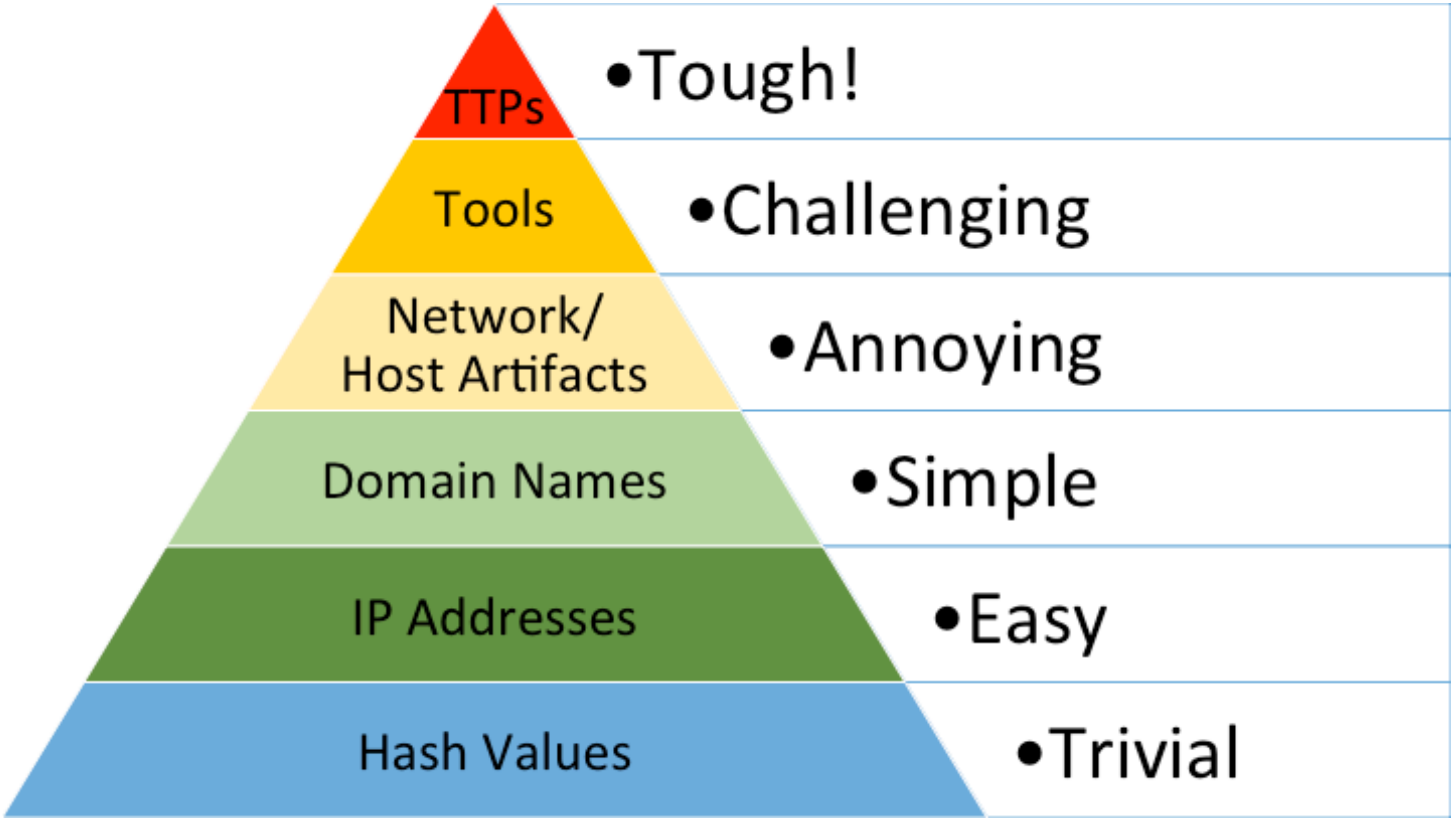
Threat feeds vs. Threat Intelligence

Threat Feeds (data enrichment)

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

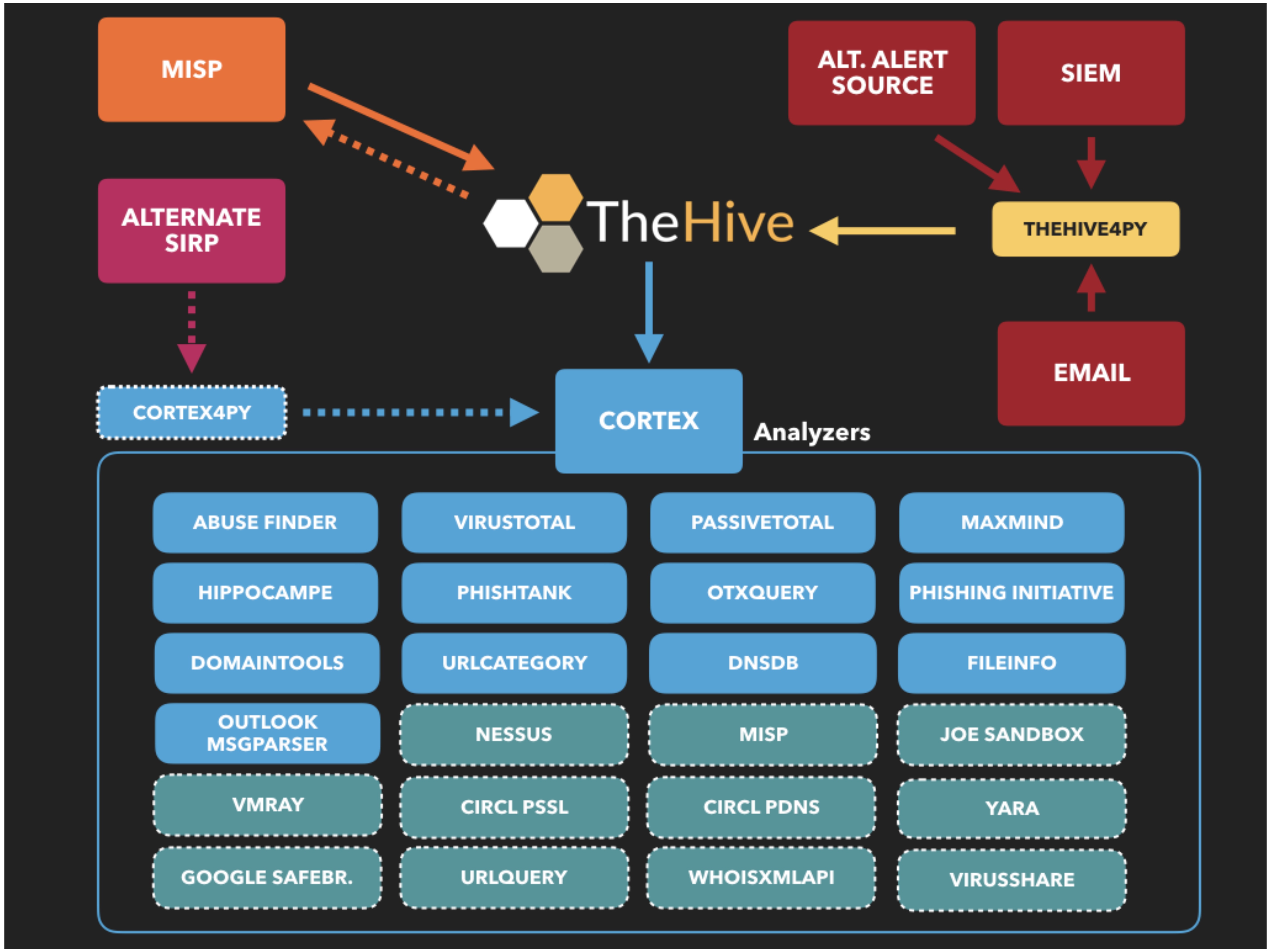
Threat Intelligence (context)

- Open Source
- Closed Source



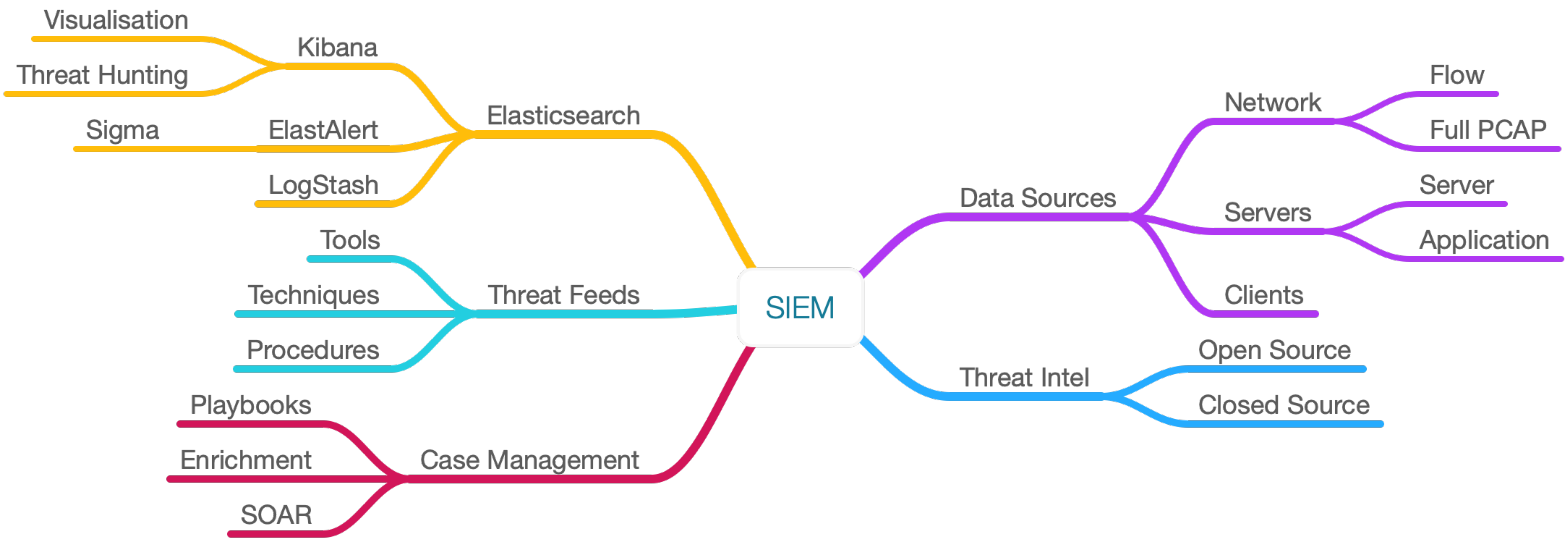
INTEGRATE! USE SOAR!

SOAR - Security Orchestration, Automation, and Response



Source: sans.org

Subject overview


Visualisation
Kibana
Threat Hunting
Elasticsearch
Sigma
ElastAlert
LogStash
Tools
Techniques
Threat Feeds
Procedures
Playbooks
Enrichment
Case Management
SOAR
SIEM
Flow
Network
Full PCAP
Data Sources
Server
Servers
Application
Clients
Open Source
Threat Intel
Closed Source