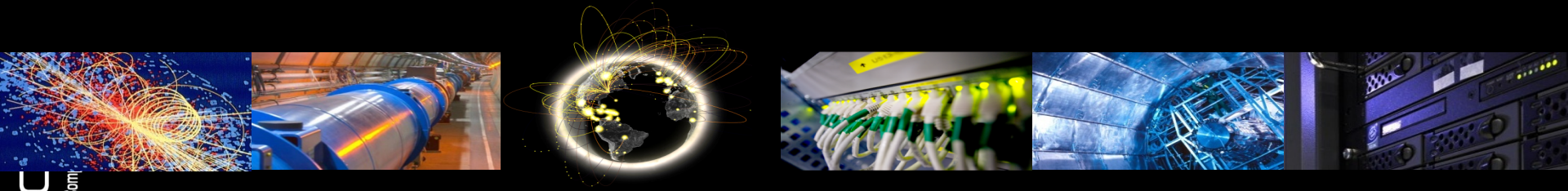
Building a minimum viable Security Operations Centre



Worldwide LHC Computing Grid

ISGC 2019, 2nd April 2019

CERN

Introduction

- Building on previous presentations at ISGC
  - 2017, 2018
- Present current status of work

WLCG SOC WG Introduction

- Working group designed to enhance site security monitoring in light of virtualized environments (including containers)
  - Network monitoring
- Coupled with threat intelligence and real time search capabilities
  - Minimally viable Security Operations Centre

Growing Scope

- Originally mandated to give guidance to WLCG sites
- Area of work enhanced by including neighbouring communities
  - NRENs
  - University CSIRTs
  - Hoping to involve EGI Fedcloud

Minimally Viable SOC

- Outcome of the Workshop during 19-21 February 2019 (hosted in UK, supported by GridPP and STFC)
  - Initial SOC model finalised and remaining steps identified
  - In particular any integrations required were identified and documentation was updated
  - https://wlcg-soc-wg-doc.web.cern.ch

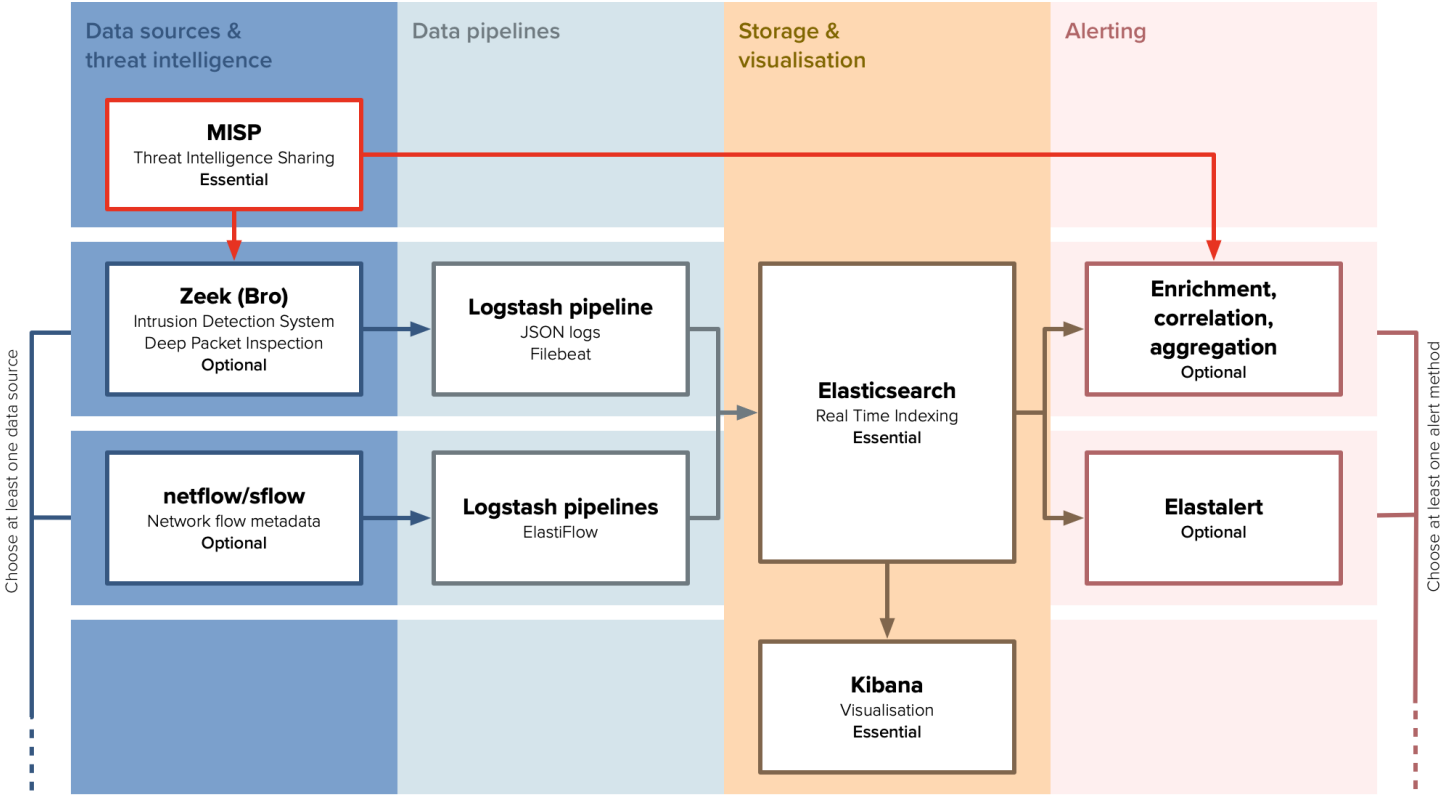
Initial Model

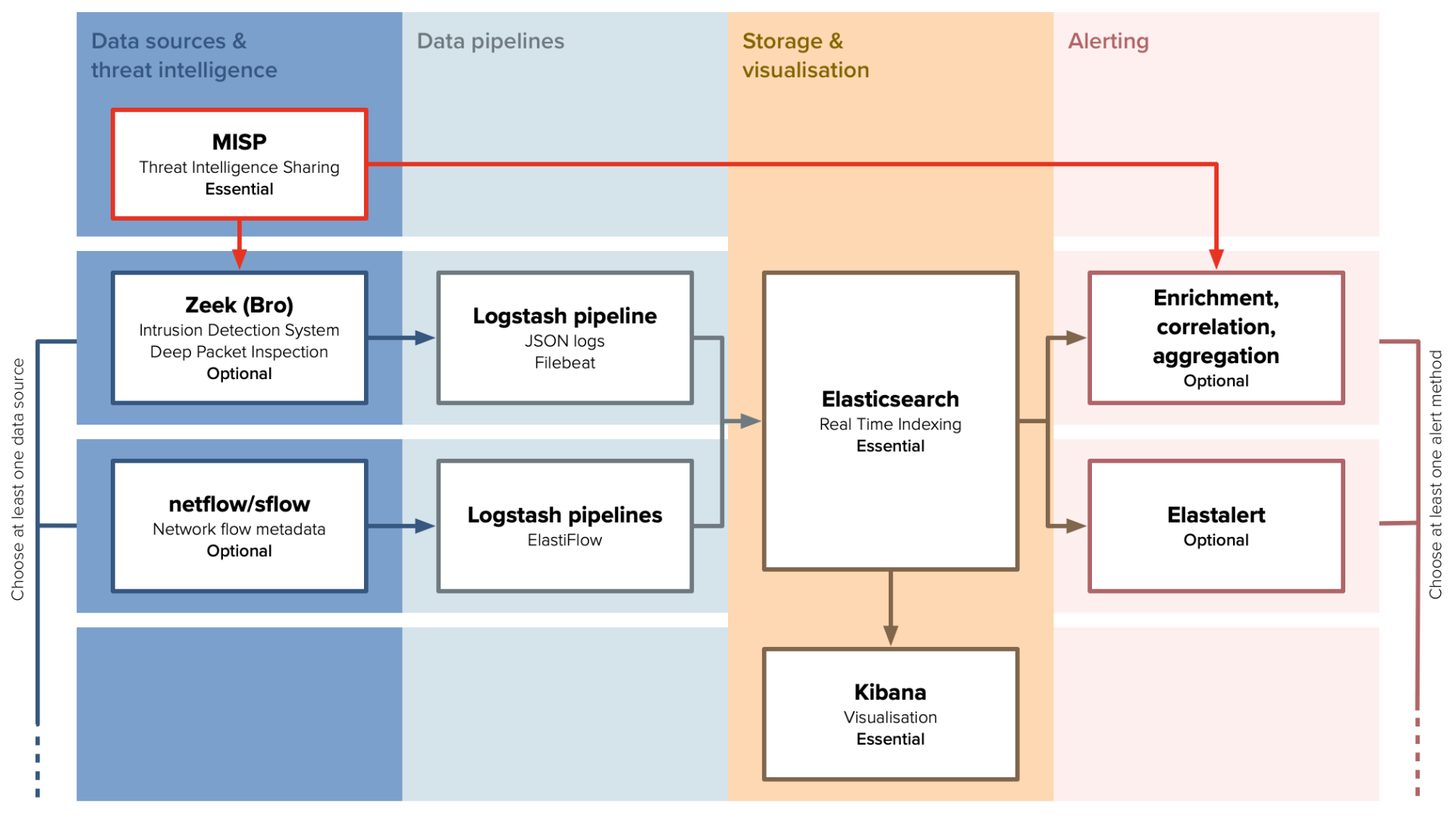
- Define 4 stages
  - Data sources
  - Threat Intelligence and pipelines
  - Storage and visualisation
  - Alerting

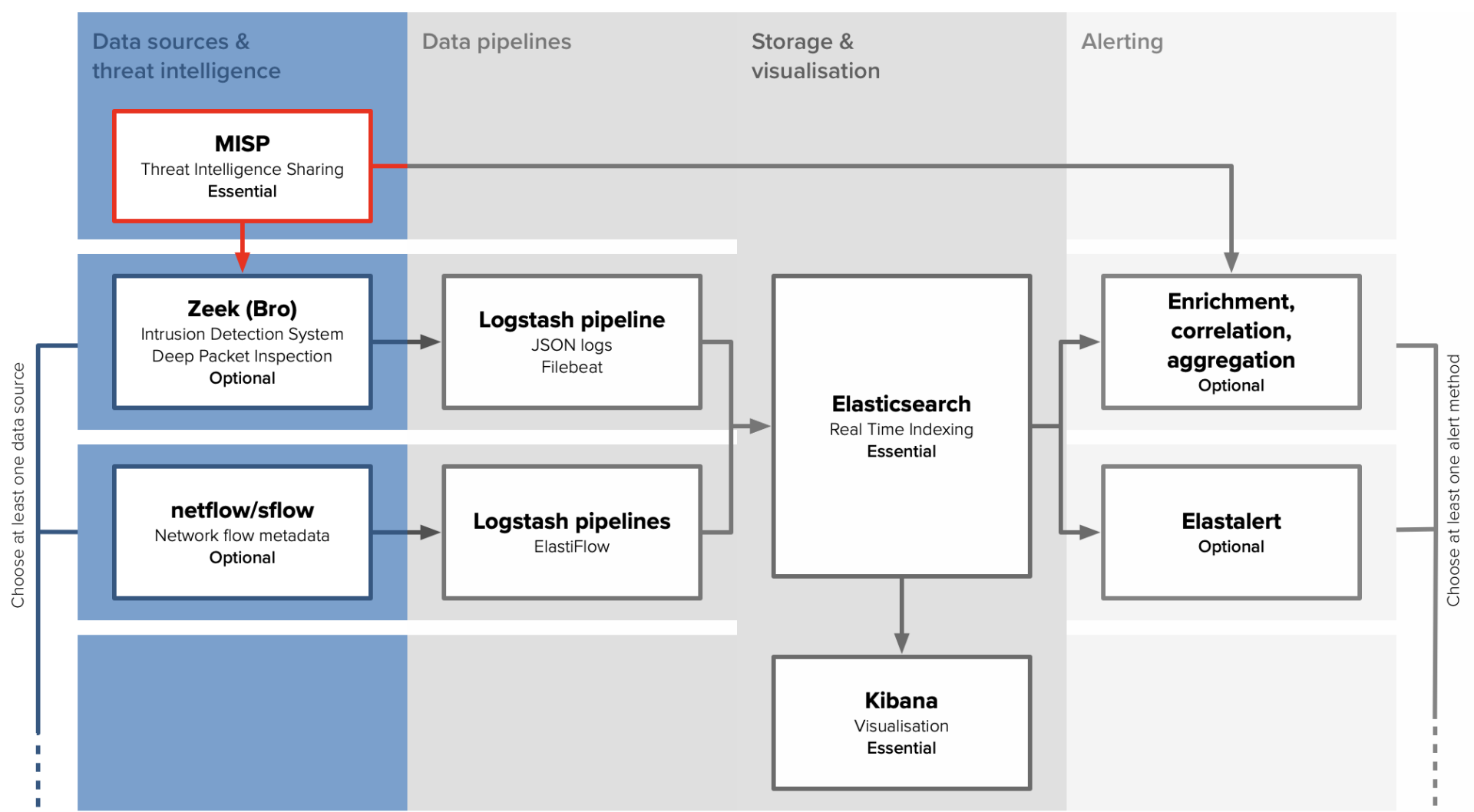
Initial Model

- Define 2 types of component
  - Essential
  - Optional (but require at least one)

Initial Model




Data sources & threat intelligence
Data pipelines
Storage & visualisation
Alerting
MISP
Threat Intelligence Sharing
Essential
Zeek (Bro)
Intrusion Detection System
Deep Packet Inspection
Optional
Logstash pipeline
JSON logs
Filebeat
netflow/sflow
Network flow metadata
Optional
Logstash pipelines
ElastiFlow
Elasticsearch
Real Time Indexing
Essential
Kibana
Visualisation
Essential
Enrichment, correlation, aggregation
Optional
Elastalert
Optional
Choose at least one data source
Choose at least one alert method


Data sources & threat intelligence
Data pipelines
Storage & visualisation
Alerting
MISP
Threat Intelligence Sharing
Essential
Zeek (Bro)
Intrusion Detection System
Deep Packet Inspection
Optional
Logstash pipeline
JSON logs
Filebeat
Elasticsearch
Real Time Indexing
Essential
Enrichment, correlation, aggregation
Optional
netflow/sflow
Network flow metadata
Optional
Logstash pipelines
ElastiFlow
Elastalert
Optional
Kibana
Visualisation
Essential
Choose at least one data source
Choose at least one alert method

Data sources & threat intelligence

- At least one of
  - Zeek (Bro): deep packet inspection
  - Netflow: network metadata
- Provide two options to hopefully cover range of use cases

Data sources

- Zeek
  - High level of information
  - Scalable and flexible
  - Dynamic protocol analysis
- However
  - Hardware implications
- Commercial options available

Data sources

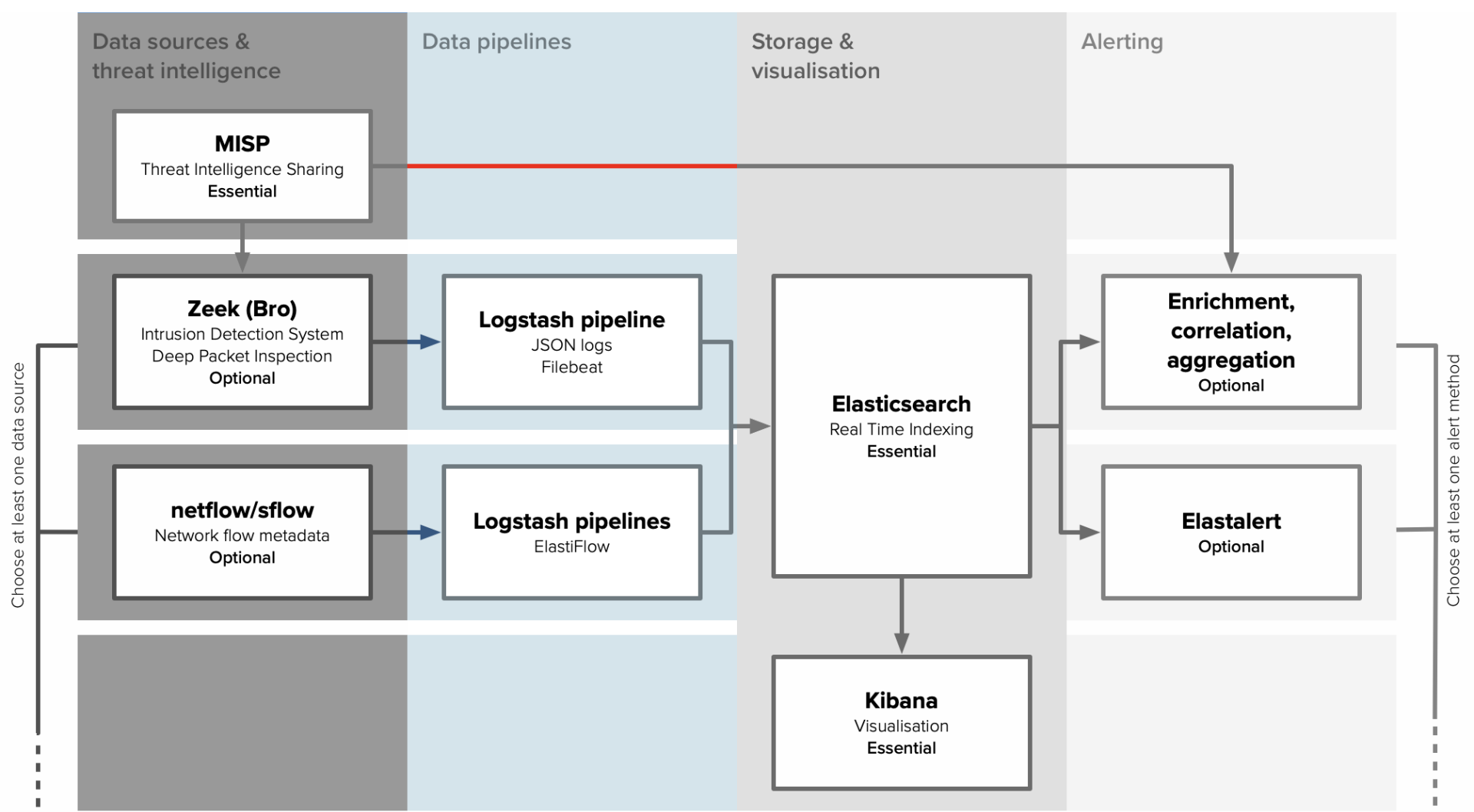
- Netflow/Sflow
  - Network metadata
  - Many switch vendors provide generators
  - Software clients
- However
  - Less data than Zeek

Threat intelligence

- Threat Intelligence
  - MISP [Essential]

Threat intelligence

- MISP
  - Essential component via web app/API access
  - Intended to sync from WLCG central instance/pull data via API
    - CERN SSO
    - Federated identity with SIRTFI or CERN Account

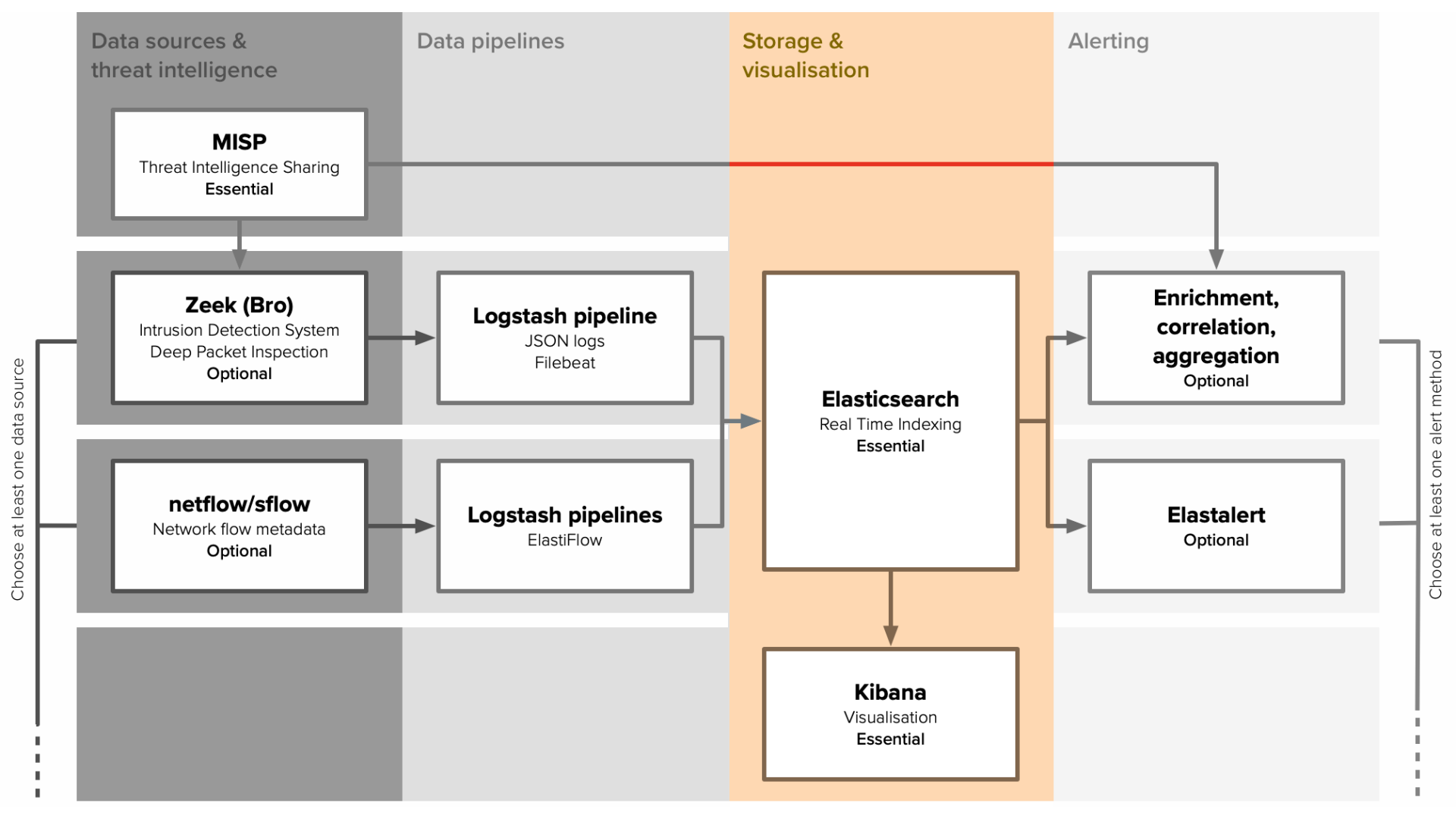

Data sources & threat intelligence
Data pipelines
Storage & visualisation
Alerting
MISP
Threat Intelligence Sharing
Essential
Zeek (Bro)
Intrusion Detection System
Deep Packet Inspection
Optional
Logstash pipeline
JSON logs
Filebeat
Elasticsearch
Real Time Indexing
Essential
Enrichment, correlation, aggregation
Optional
netflow/sflow
Network flow metadata
Optional
Logstash pipelines
ElastiFlow
Elastalert
Optional
Kibana
Visualisation
Essential
Choose at least one data source
Choose at least one alert method

Data pipelines

- Log ingestion pipelines
  - One per data source using Logstash

Pipelines

- Pipelines to ingest data into Elasticsearch
- Essential to have these matched to data sources
- Logstash
  - Well known
- Provide documentation for Zeek pipeline
- Suggest use of Elastiflow for netflow pipeline


Data sources & threat intelligence
Data pipelines
Storage & visualisation
Alerting
MISP
Threat Intelligence Sharing
Essential
Zeek (Bro)
Intrusion Detection System
Deep Packet Inspection
Optional
Logstash pipeline
JSON logs
Filebeat
Elasticsearch
Real Time Indexing
Essential
Enrichment, correlation, aggregation
Optional
netflow/sflow
Network flow metadata
Optional
Logstash pipelines
ElastiFlow
Elastalert
Optional
Kibana
Visualisation
Essential
Choose at least one data source
Choose at least one alert method

Storage and visualisation

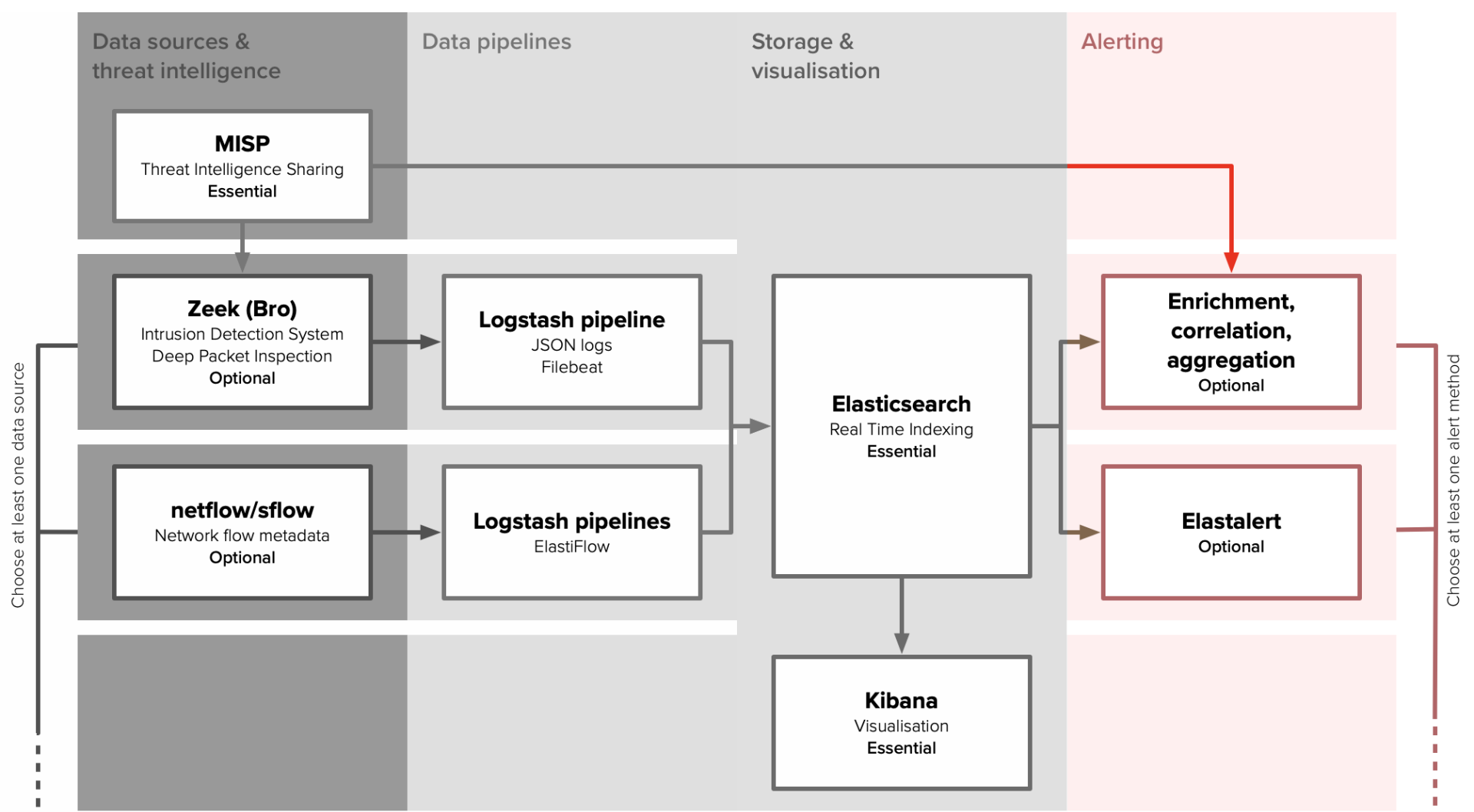
- Elasticsearch [Essential]
- Kibana [Essential]

Storage and visualisation

- Elasticsearch
  - Essential component
  - Provide deployment tips based on experience of group members

Storage and visualisation

- Kibana
  - Essential component
  - Provide some dashboards based on CERN SOC experience
  - Elastiflow provides dashboards for netflow visualisation


Data sources & threat intelligence
Data pipelines
Storage & visualisation
Alerting
MISP
Threat Intelligence Sharing
Essential
Zeek (Bro)
Intrusion Detection System
Deep Packet Inspection
Optional
Logstash pipeline
JSON logs
Filebeat
Elasticsearch
Real Time Indexing
Essential
Enrichment, correlation, aggregation
Optional
netflow/sflow
Network flow metadata
Optional
Logstash pipelines
ElastiFlow
Elastalert
Optional
Kibana
Visualisation
Essential
Choose at least one data source
Choose at least one alert method

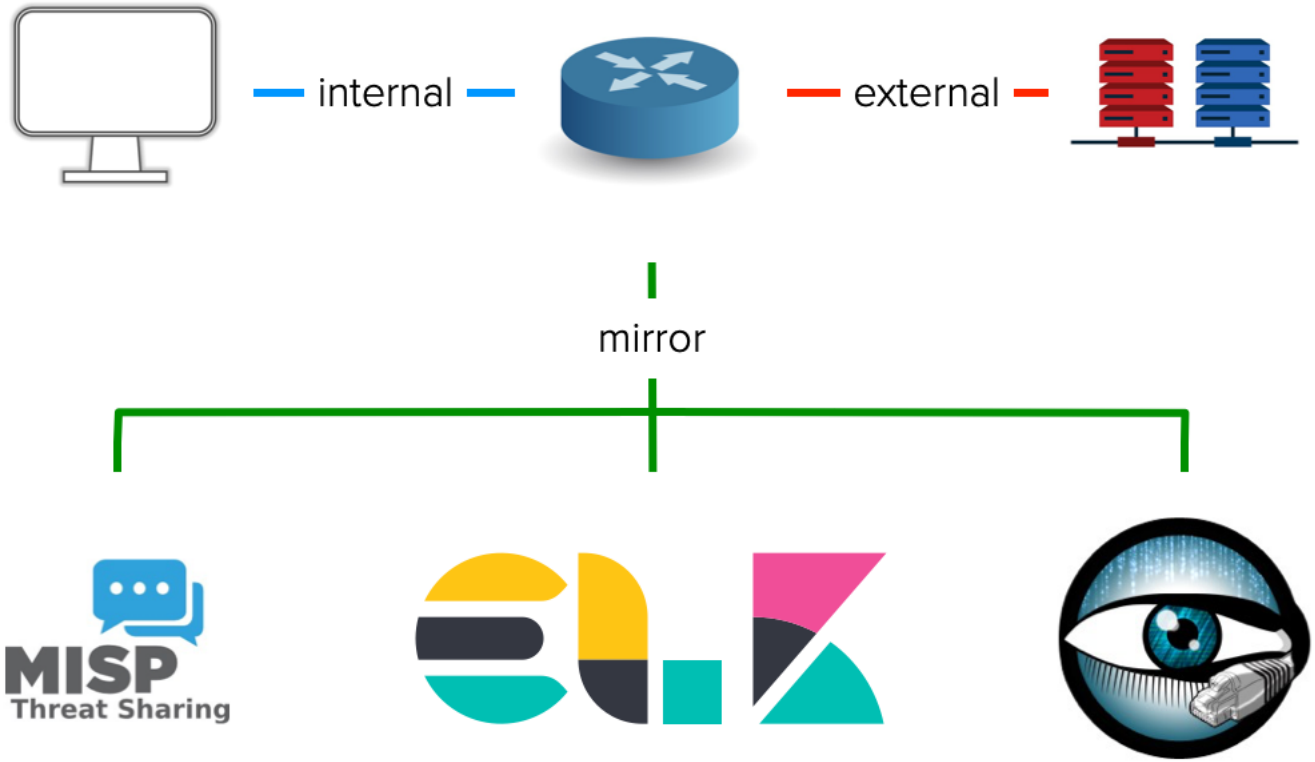
Alerting

- At least one of
  - Enrichment, correlation and aggregation scripts based on CERN example
  - Elastalert
    - Trigger on Elasticsearch query
    - Spike of events, for example

PocketSOC

- SOC demonstrator
- Docker cluster designed to run on a laptop
  - Essential components and network components
  - Minimal traffic to demonstrate workflow
  - Test new components

PocketSOC



PocketSOC

- VM made available at workshop
- In the process of a few updates then at least making it available on request
- Demo at ISGC Security Workshop on Sunday

New developments

- Project to explore a SOC deployment at Nikhef (a student working on it)
- Another project to deploy a SOC at the STFC Cloud – graduate started work
  - also working on other aspects of the Cloud
- Deployment of CERN alerting scripts at AGLT2

Immediate future

- Healthy set of actions to improve documentation
- Move select repositories outside of CERN (Github/Gitlab.com)
  - Improve access for non-CERN users
  - Make contributing as easy as possible
- Gather everything together

Immediate future

- Deployment options
  - Tightly coupled to site configuration
  - Particularly network config
  - Working on template project plan
    - Benefit from new projects
  - Look to provide somewhat automated solution for staffing constrained sites

Next few months

- Focus on threat intelligence
  - Workshop later in the year
- Validate event detection chain
  - WLCG → Site → Event detection

Final thoughts

- Fantastic to have more sites trying out deployments
- Start thinking about how we might want to deploy
- Always welcome new participants

Contact

- Main working group page
  - https://wlcg-soc-wg.web.cern.ch
- Documentation
  - https://wlcg-soc-wg-doc.web.cern.ch

Questions?