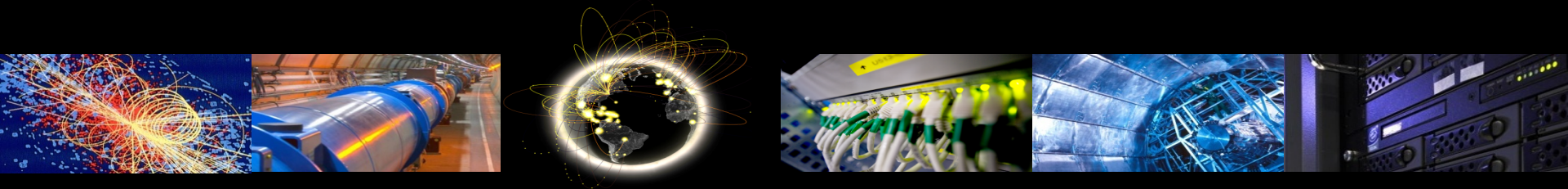


# Harnessing the power of threat intelligence for WLCG cybersecurity

WLCG Security Operations Center Working Group

*David Crooks, Liviu Vâlsan*



# Overview

- Background
- Technology stack
- Threat intelligence
- Recent progress
- Next steps
- Summary
- Contact details

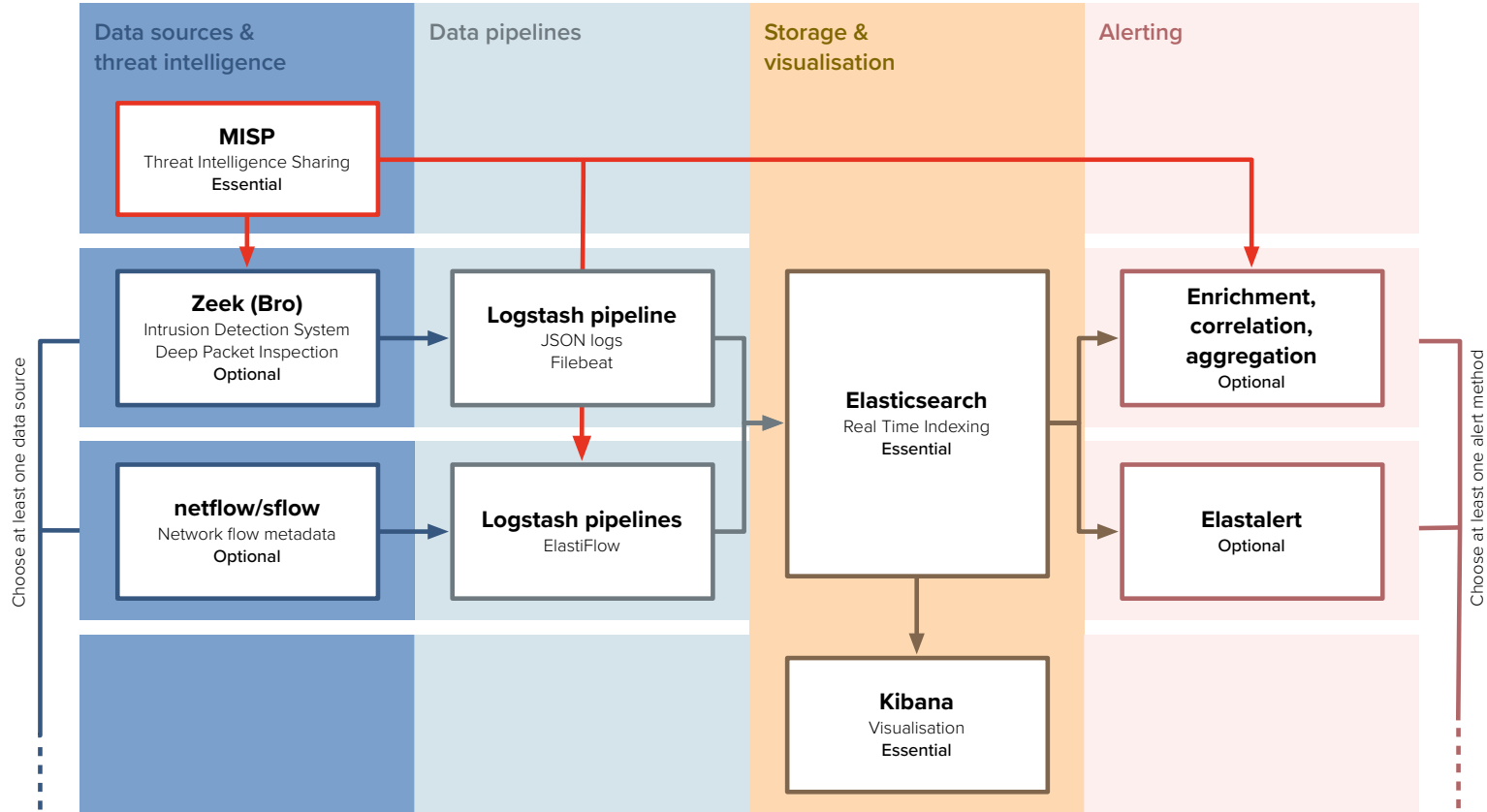
# Background

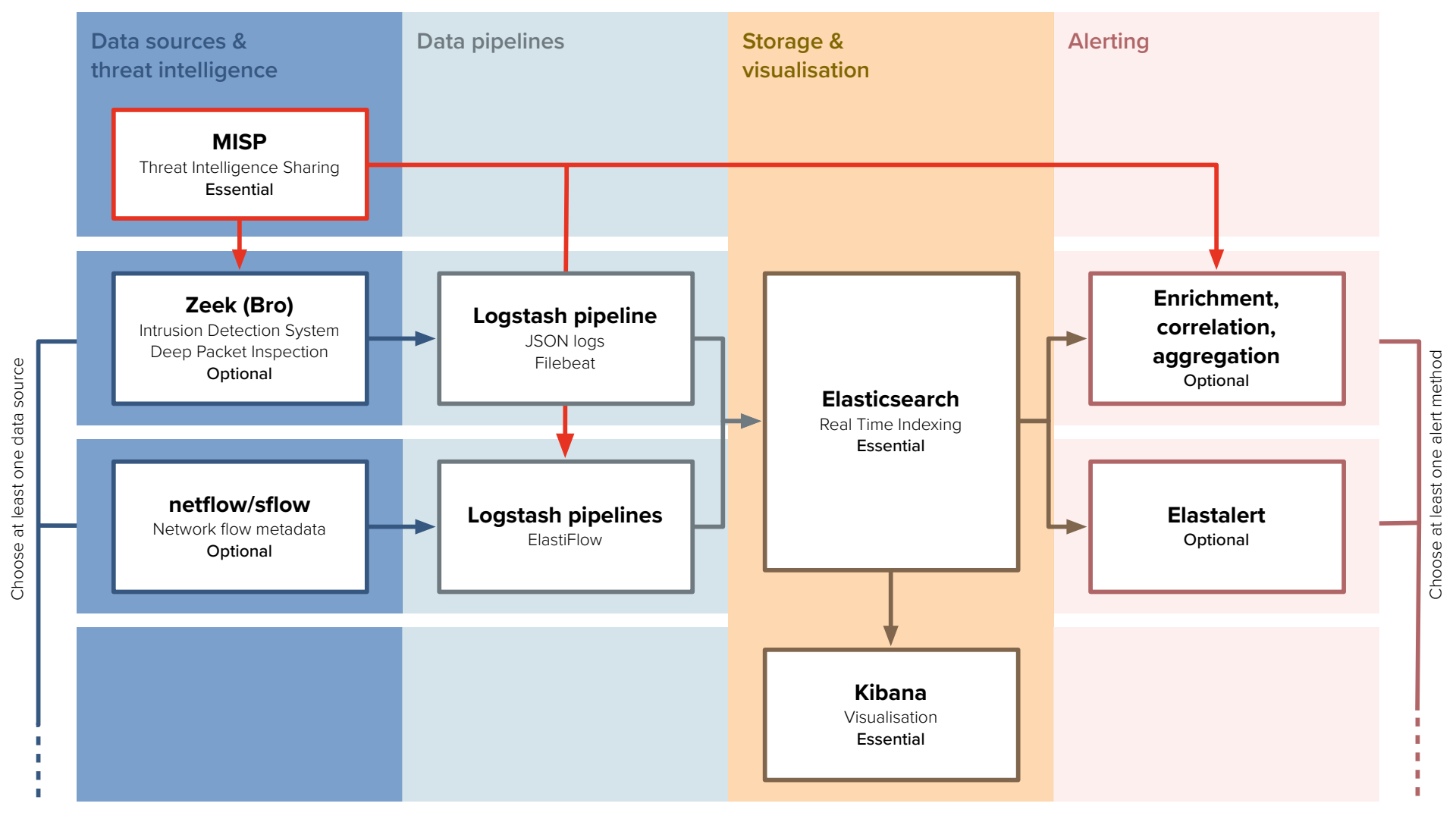
- As discussed at CHEP 2018, the WLCG SOC WG is mandated to create reference designs to allow WLCG sites to
  - Ingest security monitoring data
  - Enrich data, store and visualize
  - Alert based on matches between this security data and threat intelligence (Indicators of Compromise or *IoCs*)

# Background

- In this talk we discuss the following areas of work
  - Technology stack
  - Best practices for use and sharing of threat intelligence

# Technology stack: Initial Model





# Technology stack: initial model

Stage	Component	Notes
Threat intelligence	<a href="#">MISP</a>	Cornerstone of model; focused around central MISP instance hosted at CERN
Data sources	<a href="#">Zeek</a>	Highly detailed but requires dedicated hardware
	<a href="#">Netflow</a>	Readily available at many sites but offers less information than Zeek
Data pipelines	<a href="#">Logstash</a> + <a href="#">Filebeat</a> + JSON logs (e.g. Zeek)	Basic pipeline provided by WG
	<a href="#">Logstash</a> + <a href="#">Elasticflow</a> (Netflow)	Dedicated pipeline for netflow/sflow
Storage and Visualisation	<a href="#">Elasticsearch</a>	Share deployment configs within group
	<a href="#">Kibana</a>	Share dashboard processes
Alerting	<a href="#">Correlation scripts</a>	Generalised version of CERN scripts
	<a href="#">Elastalert</a>	Rule based alerts; share typical configs

# Recent progress

- This summer, two new SOC prototypes under development:
  - Nikhef: Zeek data source (OpenPOWER8)
  - STFC Cloud: sFlow from subset of hypervisors
- At the recent [SOC Workshop](#) in Nikhef (21-21 October), demonstrated SOC workflow:
  - Trigger activity at CERN (using EGI CSIRT SSC framework)
    - Create MISP event
  - Check the propagation of this threat intelligence to STFC
  - Trigger same activity at STFC
    - Check this is seen/alerted on
- Successful demonstration and important milestone



# Threat intelligence

- So far have discussed technology stack
  - Built a reference design
  - Initial deployments
  - Technology test of workflow
- What about threat intelligence itself?

# Threat intelligence

- Important to have highly focused, relevant intelligence
  - Guidelines on what types of indicators to include
  - As specific as possible, *including context*
- What process do we use to sync intelligence between sites?
  - Focus on CERN instance as central hub
  - Access to other sites via separate MISP instances or direct API access
    - Anticipate many sites would use direct access
    - Explore tiered approach using UK instance (in development at STFC): c.f. Argus

# Best practices

- Lots of discussion at the recent SOC Workshop
  - How best to make use of threat intelligence shared via central MISP instance hosted at CERN
  - Including WLCG and other scientific communities
- How does a site gain access to intelligence?
- What is expected of them?
  - Code of conduct
  - For example: respect TLP
- Maintaining high level of trust between participants sharing information is paramount

# Code of conduct: TLP

LEVEL	DEFINITION
<b>RED</b>	Not for disclosure, restricted to participants only
<b>AMBER</b>	Limited disclosure, restricted to participants' organizations
<b>GREEN</b>	Limited disclosure, restricted to the community
<b>WHITE</b>	Disclosure is not limited

# Threat intelligence & operational security

- Lead to clarification of role of WG
- Draw a distinction between
  - the technologies, infrastructure and best practice used to share threat intelligence (focus of WG)
  - the threat intelligence itself and actual sharing of information in the course of operational security

# Security Operations

- The CERN MISP instance is aimed at WLCG sites
  - Including campus/institution teams for those sites
- For other communities, please contact
  - [wlcg-security-officer@cern.ch](mailto:wlcg-security-officer@cern.ch)
- CERN instance designed to be open
  - **But** governed by strict rules of access to increase trust
- Document on guidelines for access to CERN instance to be prepared this year

# Deployment options

- How might we suggest proceeding with a wider roll out of this capability?
- Current direction is towards encouraging participation particularly within Tier-1s
- Envisage a focus by the WG on assisting individual sites with deployment
  - Any volunteers?

# Next steps

- Consideration of usage models at different sites (Tier-1s vs Tier-2s, for example)
  - Staffing implications
  - Additional components
- Continued work on existing deployments
  - And hopefully adding more participants!



# Summary

- Progress made on adding initial capability to more sites
- During recent workshop, demonstrated SOC workflow
  - Important milestone
- Clarification of role of WG
  - Moving forward with how sites from different communities can access threat intelligence

# Contact details

- Website
  - [wlcg-soc-wg.web.cern.ch](http://wlcg-soc-wg.web.cern.ch)
- Documentation
  - [wlcg-soc-wg-doc.web.cern.ch](http://wlcg-soc-wg-doc.web.cern.ch)
- Egroup
  - [wlcg-soc-wg@cern.ch](mailto:wlcg-soc-wg@cern.ch)
- David Crooks ([david.crooks@cern.ch](mailto:david.crooks@cern.ch))
- Liviu Vâlsan ([livi.ivalsan@cern.ch](mailto:livi.ivalsan@cern.ch))
- Access to CERN MISP
  - [wlcg-security-officer@cern.ch](mailto:wlcg-security-officer@cern.ch)