Science and
Technology
Facilities Council

Sharing Threat Intelligence

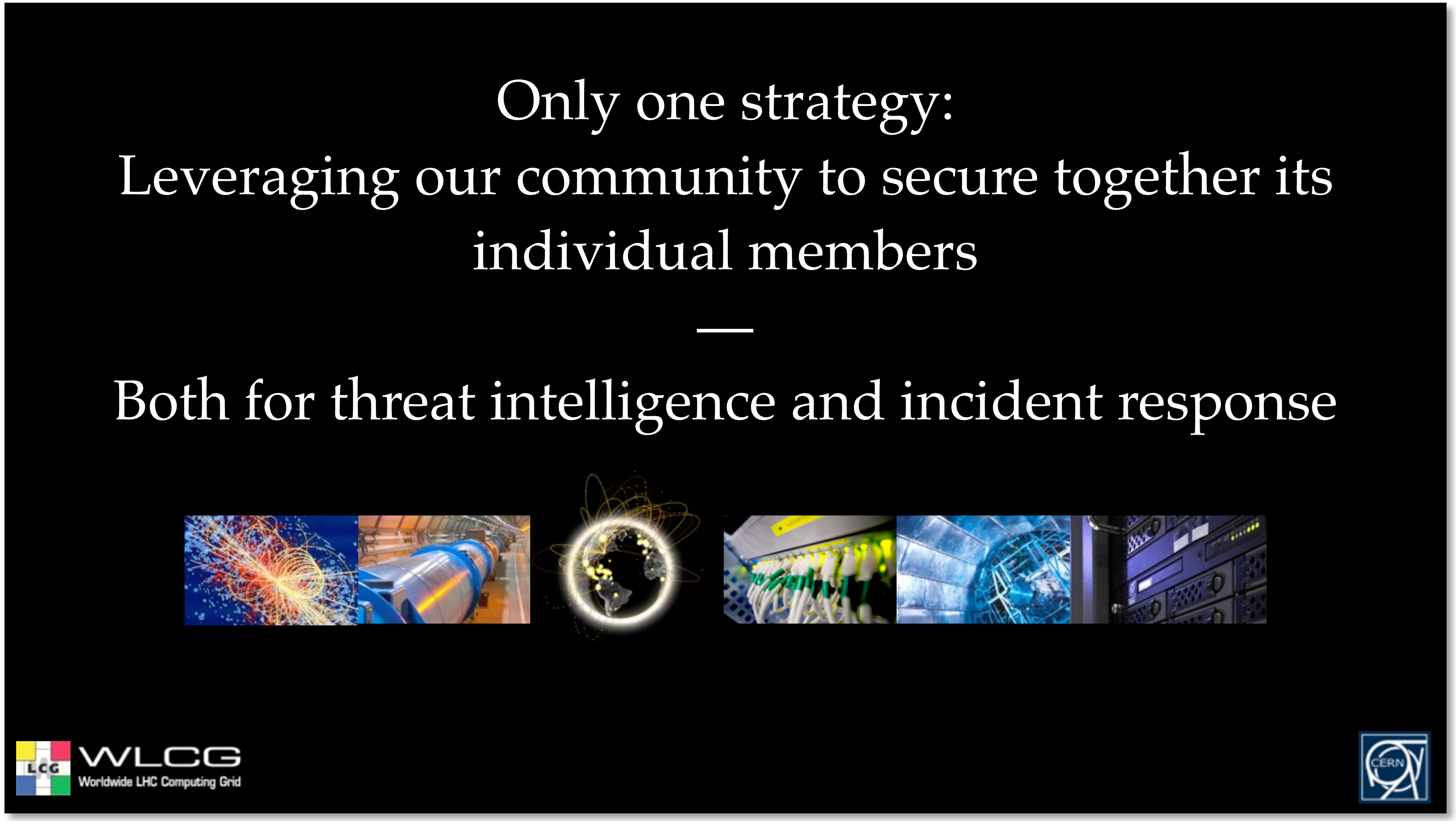
David Crooks
david.crooks@stfc.ac.uk

Landscape

- The research and academic community face a range of shared threats
  - As we are well aware

- Both directed at infrastructure, and particularly via social engineering
  - Phishing is a perhaps the largest threat we face
  - Credential theft and resale is widespread: there is money to be made
  - Subject to attacks from cybercriminals (opportunistic and targeted) and as collateral damage in nation-state attacks

Landscape



Only one strategy:
Leveraging our community to secure together its individual members

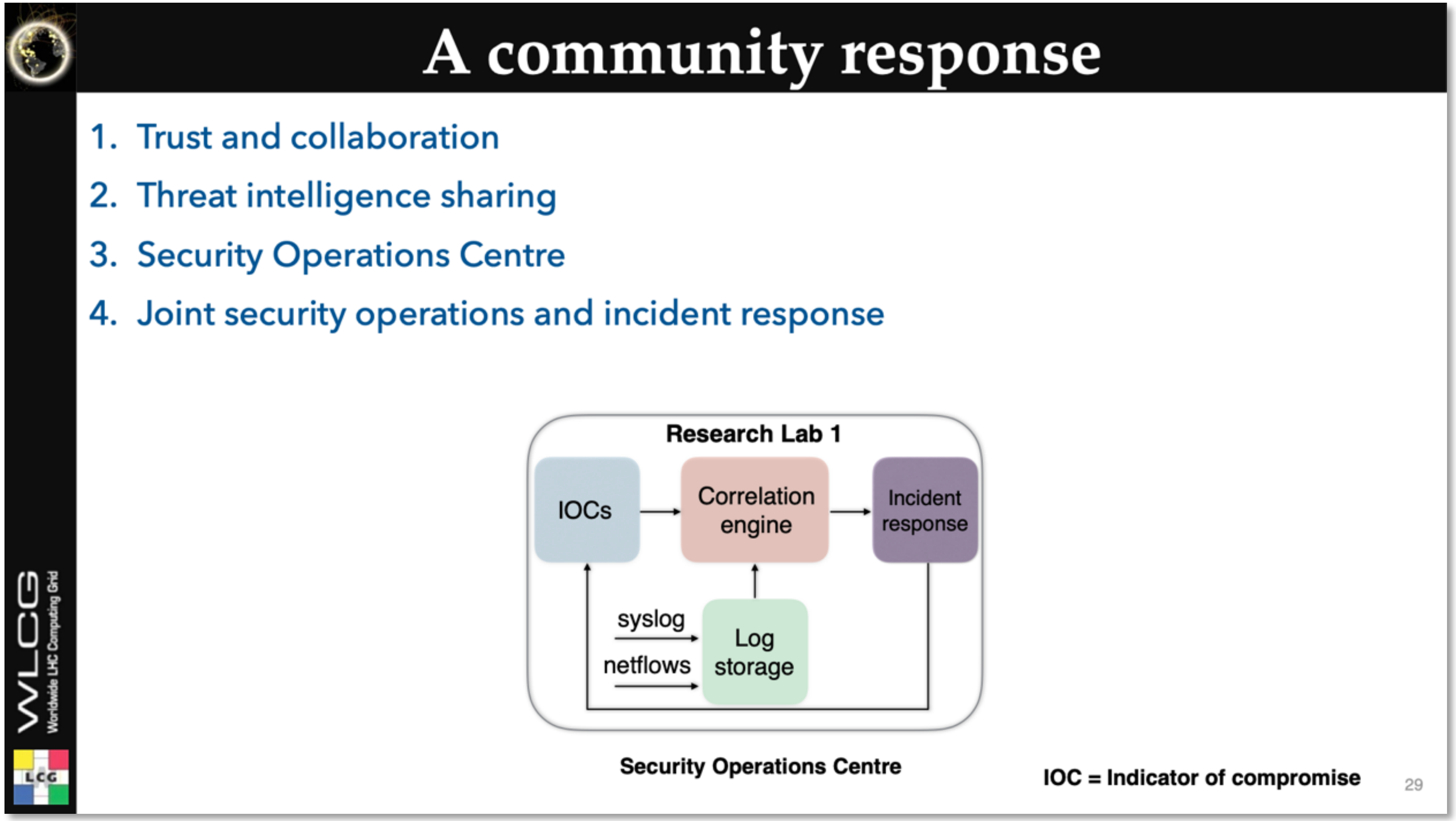
—

Both for threat intelligence and incident response

Romain Wartel (Worldwide LHC Computing Grid Security Officer)

Tackling modern cyberthreats together is the only way forward
Computing for High Energy Physics 2019, Adelaide, Australia, November 2019

Landscape



A community response

1. Trust and collaboration
2. Threat intelligence sharing
3. Security Operations Centre
4. Joint security operations and incident response

Research Lab 1

IOCs → Correlation engine → Incident response

syslog, netflows → Log storage → Correlation engine

Security Operations Centre

IOC = Indicator of compromise

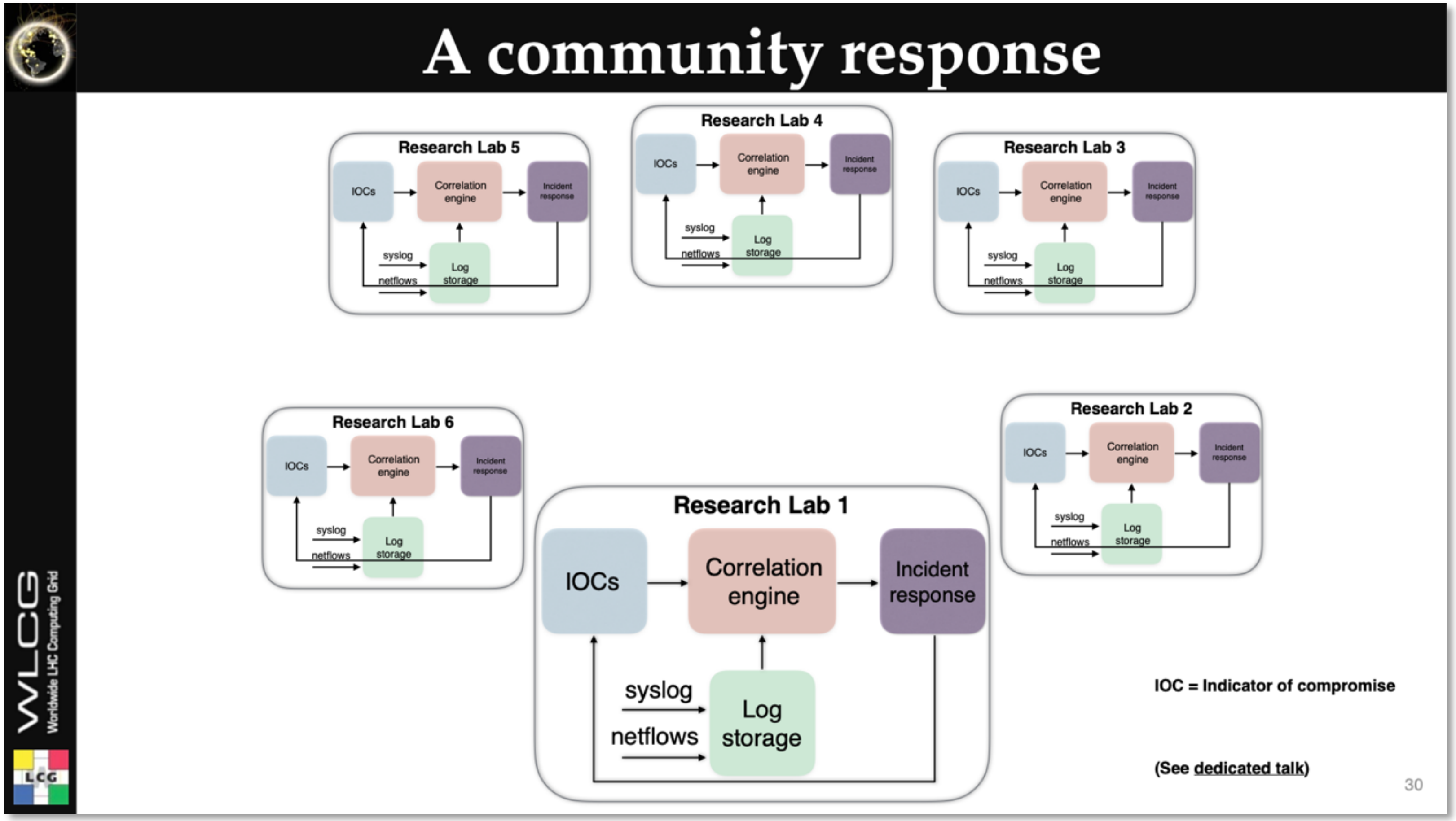
WLCG Worldwide LHC Computing Grid

Romain Wartel (Worldwide LHC Computing Grid Security Officer)

Tackling modern cyberthreats together is the only way forward

Computing for High Energy Physics 2019, Adelaide, Australia, November 2019

Landscape



A community response

Research Lab 5

IOCs → Correlation engine → Incident response

syslog, netflows → Log storage

Research Lab 4

IOCs → Correlation engine → Incident response

syslog, netflows → Log storage

Research Lab 3

IOCs → Correlation engine → Incident response

syslog, netflows → Log storage

Research Lab 6

IOCs → Correlation engine → Incident response

syslog, netflows → Log storage

Research Lab 1

IOCs → Correlation engine → Incident response

syslog, netflows → Log storage

Research Lab 2

IOCs → Correlation engine → Incident response

syslog, netflows → Log storage

IOC = Indicator of compromise

(See dedicated talk)

Science and Technology Facilities Council

iris

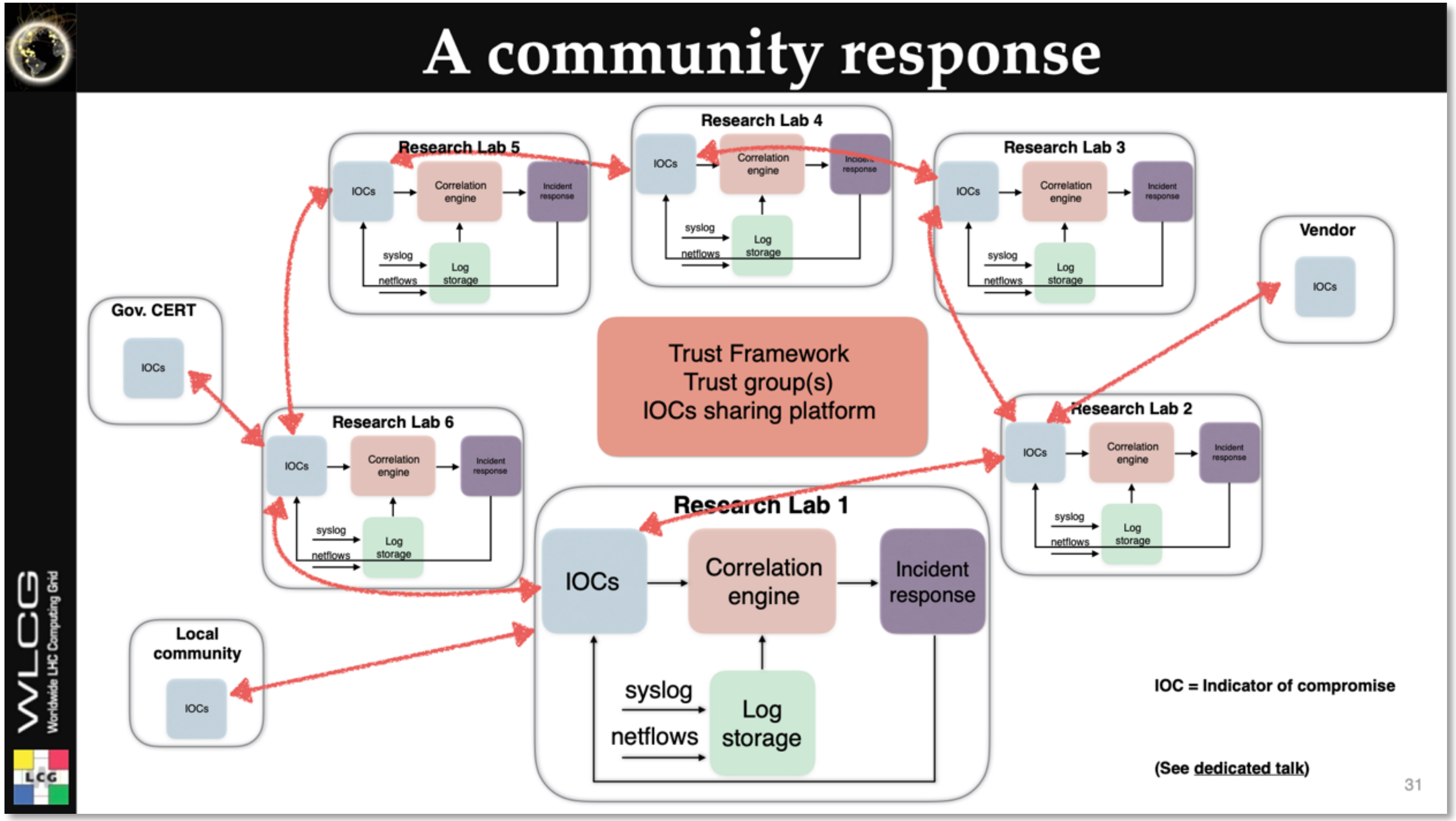
CSIRT

WISE COMMUNITY

Romain Wartel (Worldwide LHC Computing Grid Security Officer)

Tackling modern cyberthreats together is the only way forward
Computing for High Energy Physics 2019, Adelaide, Australia, November 2019

Landscape



A community response

IOC = Indicator of compromise

(See dedicated talk)

31

Romain Wartel (Worldwide LHC Computing Grid Security Officer)

Tackling modern cyberthreats together is the only way forward

Computing for High Energy Physics 2019, Adelaide, Australia, November 2019

Threat intelligence

- Communication between academic security teams and representatives is vital

- However: since we see similar attacks, we can share intelligence

- Allowing WLCG sites to digest and make active use of threat intelligence is a cornerstone of the WLCG security strategy

Active use of intelligence

- In order to use this intelligence, we need

- Methods to share intelligence
- The right people to have access to make best use of the data
- Methods to act on intelligence and apply it to a particular site

WLCG SOC WG

- The WLCG Security Operations Centre WG was established to enable the deployment of security tools to enable this
  - But also including members from the wider academic research community
- The working group is mandated to create reference designs to allow sites to
  - Ingest security monitoring data
  - Enrich, store and visualize this security data
  - Alert based on matches between the stored data and threat intelligence
    - Indicators of Compromise or IoCs
- A deployment of such a design is a Security Operations Centre (SOC)

Active use of intelligence

- In order to use this intelligence, we need

- **Methods to share intelligence**
- The right people to have access to make best use of the data
- Methods to act on intelligence and apply it to a particular site

Academic MISP instance

- Intelligence sharing model using MISP platform [misp-project.org]
- Hub and spoke based around instance hosted at CERN
  - Benefit from CERN trust relationships and experience
- Mostly TLP:GREEN and TLP:WHITE
  - Information that is limited to the community or public
- TLP:AMBER events produced by CERN
  - Information that should only be shared with trusted security contacts

Academic MISP instance

- We have a prototype STFC MISP instance which syncs data from CERN
- Access granted via IRIS-IAM
- Testing now with small number of security contacts
  - Including STFC Information Security
  - Collaboration to integrate with their systems
  - Access via web or API
- Ongoing work on how to incorporate this workflow into the incident response procedures of operational teams

Active use of intelligence

- In order to use this intelligence, we need a few things

- Methods to share intelligence
- **The right people need access to make best use of the data**
- Methods to act on intelligence and apply it to a particular site

Access to threat intelligence

- Threat intelligence shared via CERN was originally intended for use by WLCG sites (including GridPP) and their host institutions
  - Clear interest in extending that to other academic domains
- Rules of participation document has been drafted for other communities
  - Including IRIS
- Focused on honouring sharing restrictions
  - I have agreed in principle for IRIS (I also helped in the drafting)
- Not part of a large scale rollout at this stage, but part of ongoing development
  - Focused on resource providers – expressions of interest welcome!

Institutional teams

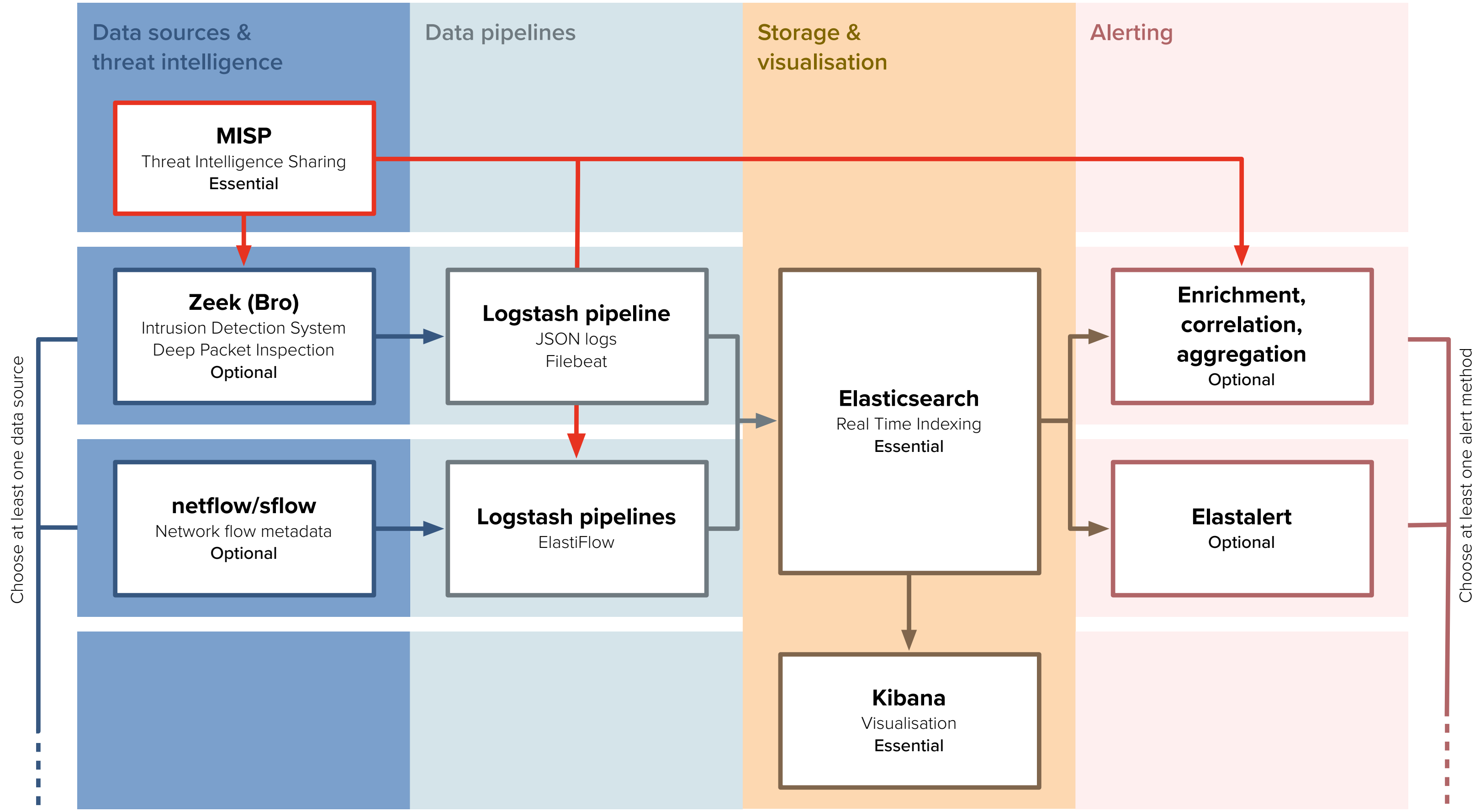
- Institutional security teams are key to this process
- Much of the information is particularly useful at that level
  - Details of phishing campaigns, etc.
- Particular aspect of this work has been the relationship between grid sites and campus teams
  - How is this relationship for HPC and Cloud providers?

Active use of intelligence

- In order to use this intelligence, we need a few things

- Methods to share intelligence
- The right people need access to make best use of the data
- **Methods to act on intelligence and apply it to a particular site**

WLCG SOC WG



Science and Technology Facilities Council

WLCG SOC WG

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

Science and Technology Facilities Council

STFC Cloud SOC

- Prototype system in place for STFC Cloud
  - Ingest network metadata from subset of Cloud hypervisors
  - Enrich this with event data from MISP
  - Store in Elasticsearch
  - Alert based on correlations
- In operation at a limited scale, but live
- Same API used for this can be used to give access for other systems
  - Including STFC Information Security

Current wider status

- End-to-end test of intelligence sharing workflow
  - Generate MISP event at CERN based on “malicious traffic”
  - Shared this with STFC prototype and demonstrate that this causes alert based on same traffic
- Working with several prototype systems
  - In addition to production, fully featured SOC at CERN
- For WLCG, focus on supporting Tier-1 sites in deploying these tools
  - Biggest impact of having sharing in place

Conclusion

- Collaborating on operational security is vital
- Sharing threat intelligence is a cornerstone of WLCG security development
  - I would extend this to IRIS
- Intelligence is available, along with reference designs on how to use it
  - Integrating with existing monitoring where appropriate
- Interest in taking part in testing very welcome!

Science and
Technology
Facilities Council

Questions?

Science and Technology Facilities Council

Thank you

Science and Technology Facilities Council   @STFC_Matters   Science and Technology Facilities Council