SOC Working Group:
Threat Intelligence Sharing

David Crooks
david.crooks@glasgow.ac.uk

for the WLCG SOC Working Group

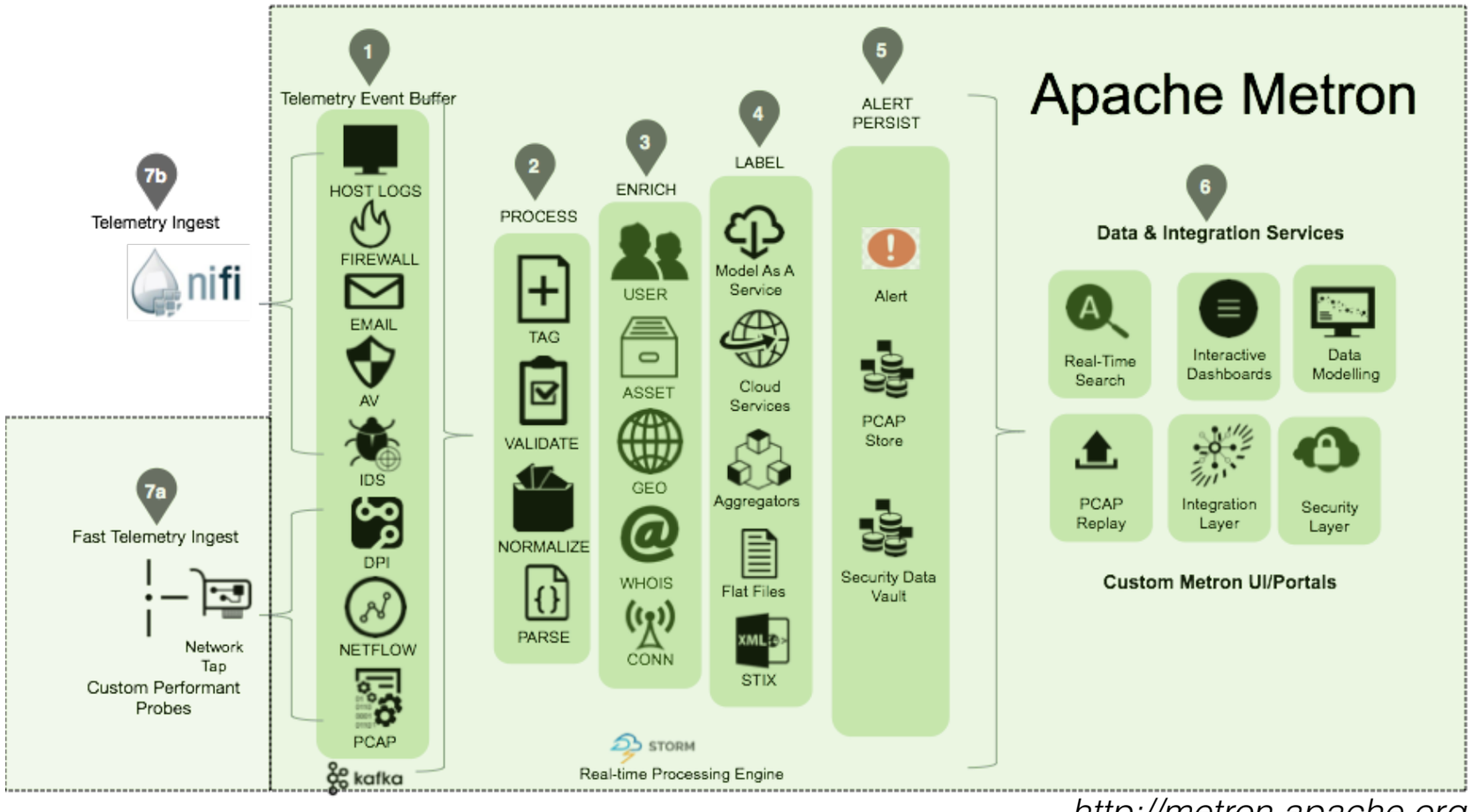
GridPP39, September 2017

SOC Working Group Status

- Update on the work of the SOC Working Group
- Specific area where GridPP can contribute

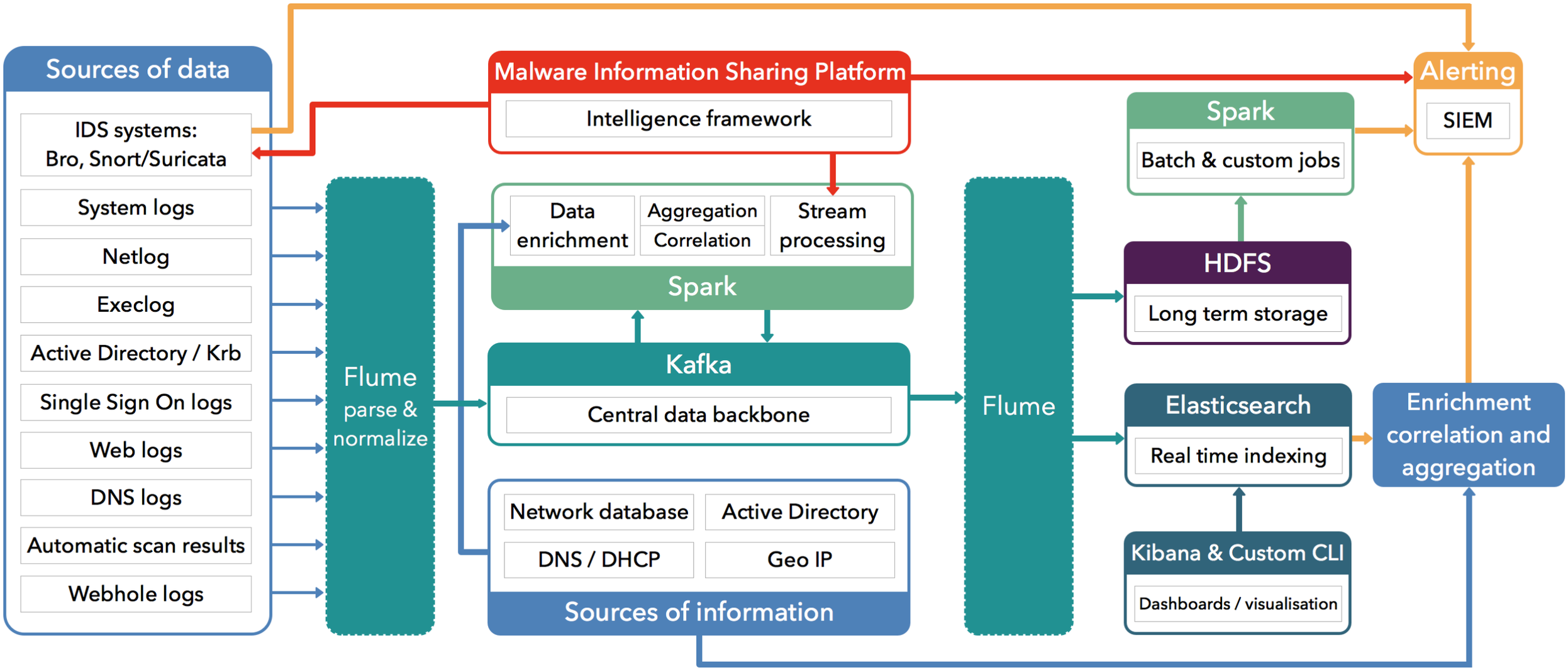
Security Operations Centres

- SOCs can be very complex, employing a large number of tools



http://metron.apache.org

CERN SOC


Sources of data
IDS systems:
Bro, Snort/Suricata
System logs
Netlog
Execlog
Active Directory / Krb
Single Sign On logs
Web logs
DNS logs
Automatic scan results
Webhole logs
Flume
parse & normalize
Malware Information Sharing Platform
Intelligence framework
Data enrichment
Aggregation
Correlation
Stream processing
Spark
Kafka
Central data backbone
Network database
Active Directory
DNS / DHCP
Geo IP
Sources of information
Flume
Alerting
SIEM
Spark
Batch & custom jobs
HDFS
Long term storage
Elasticsearch
Real time indexing
Kibana & Custom CLI
Dashboards / visualisation
Enrichment correlation and aggregation

CERN SOC

- 100s of GB/day
- Varied range of data
- Built on top of existing CERN IT services whenever possible
- Lessons for other sites (while not necessarily at the same scale)

Technologies

- Given complexity, how best to proceed?
- Minimum viable product
  - What set of tools is effective and allows growth?
- Intrusion Detection System (IDS)
  - Bro
- Threat Intelligence
  - Malware Information Sharing Platform (MISP)

Bro

- *"Bro is an open-source network security platform that illuminates your network's activity in detail, with the stability and flexibility for production deployment at scale."*
- Strong use in the US
- bro.org
- Act as partner to MISP

Bro

- Scalable
  - Build Bro cluster with worker nodes to expand capabilities
- Important part of work to explore requirements for different sizes and types of sites
  - Network topology
- Part of scalability is running multiple instance of Bro across network interface
  - PF_RING (http://www.ntop.org/products/packet-capture/pf_ring/)

Bro status

- **Brunel**
  - Working with CISCO Nexus switches/ Netflow
- **Lancaster**
  - Planning to test deployment with CERN RPMs
- **Durham**
  - Lenovo nx360 - 40 HT cores
  - On-switch network mirroring 4Gb/s WAN link
  - 10 GB/day logs raw, run periodically as degrades overall network performance
- **Glasgow**
  - DELL C6145 - 64 cores
  - On-switch network mirroring 10 Gb/s WAN link
  - 250-300 GB/month (compressed)
- **Oxford**
  - DELL R610 - 16 cores
  - Initial installation
- **Edinburgh**
  - Planned installation

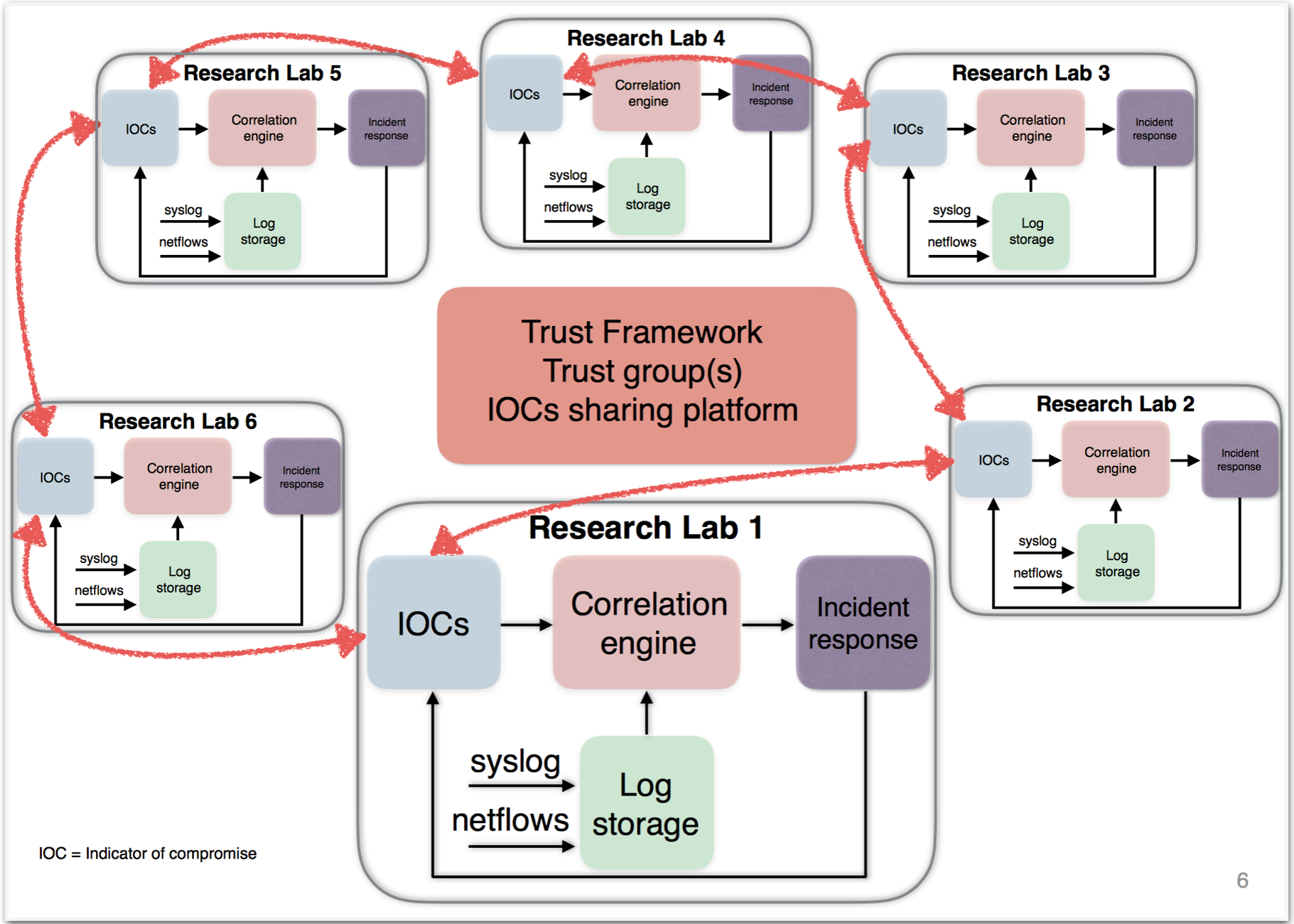
Threat Intelligence

- As a community, threats apply to us all - shared responsibility

- Need to share intelligence to improve ability to respond in a timely fashion

- *The future of academic security (Romain Wartel)*
  - http://indico.cern.ch/event/505613/contributions/2227689/attachments/1349009/2047093/Oral-109.pdf

Threat Intelligence



Romain Wartel

http://indico.cern.ch/event/505613/contributions/2227689/attachments/1349009/2047093/Oral-109.pdf

MISP

- Malware Information Sharing Platform

- *"A platform for sharing, storing and correlating Indicators of Compromises of targeted attacks. Not only to store, share, collaborate on malware, but also to use the IOCs to detect and prevent attacks."*

- Allows development of trust frameworks between sites to allow rapid sharing of threat intelligence

- misp-project.org

MISP Status

- Installed at Glasgow; work at RAL last year
- In Glasgow used to share WLCG data with local campus security (early investigation) - sync data with CERN credentials, then give local access to campus personnel
- Investigations at other sites including Edinburgh

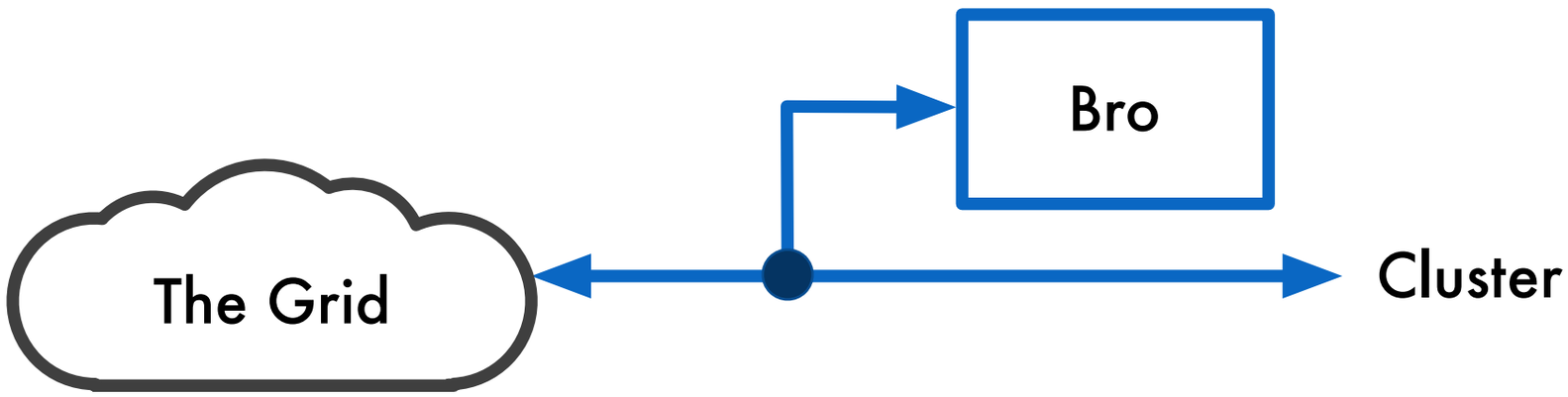
WLCG MISP

- WLCG MISP, in place at CERN, accessible once added as a user with CERN credentials, and to institutions with Sirtfi enabled IdPs.

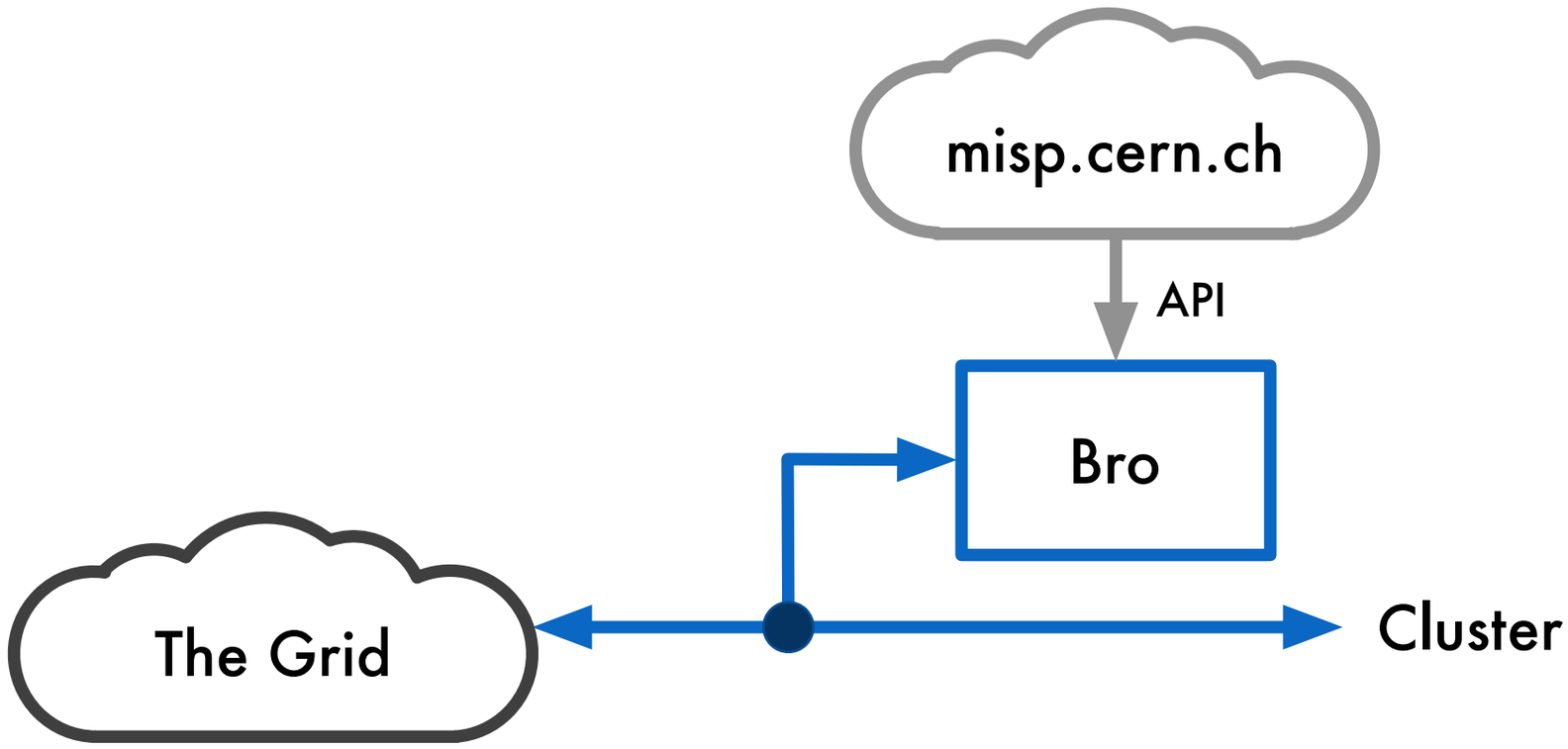
- misp.cern.ch
  - 3805 events
  - 261662 attributes
  - from 190 different organisations

Simple model

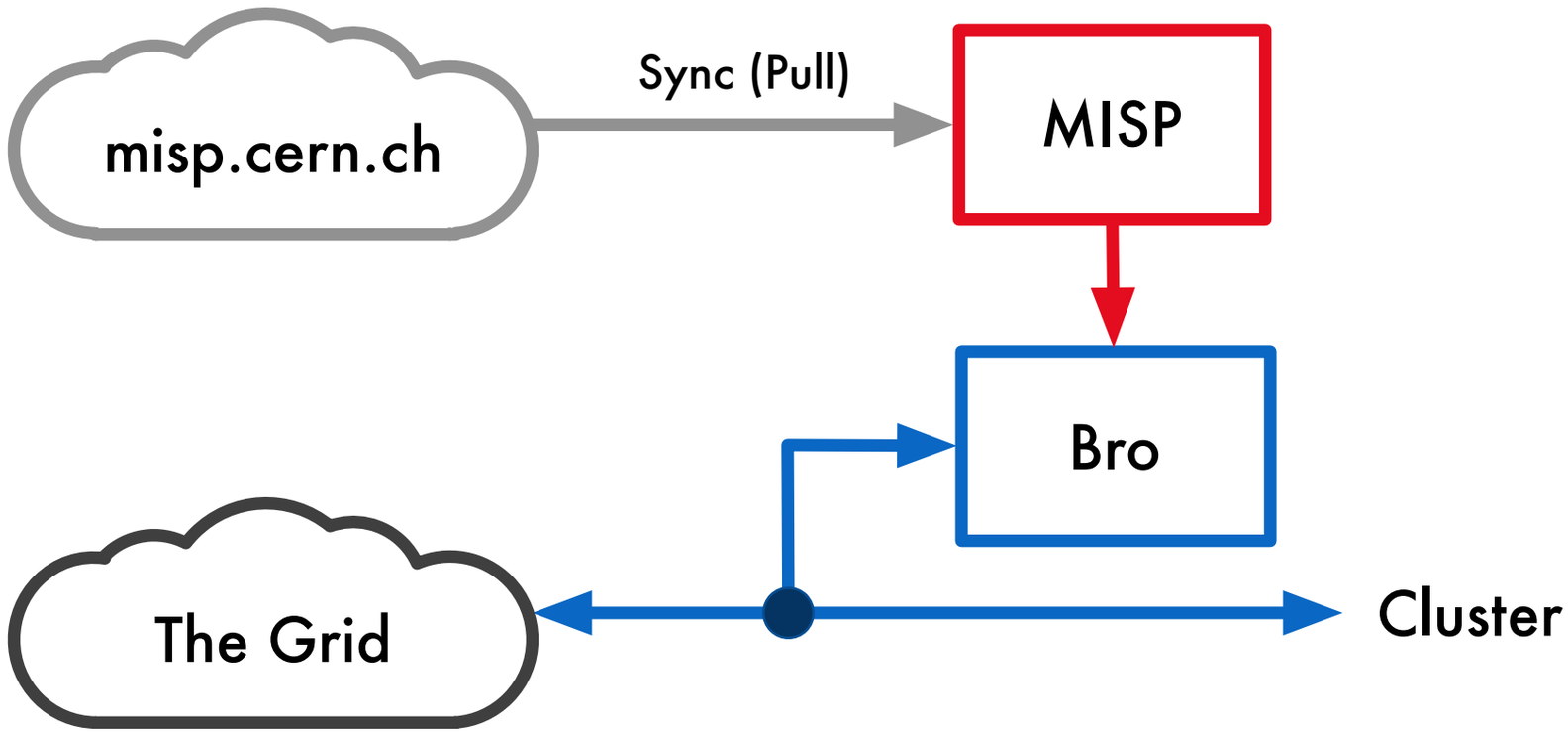
Simple model



Simple model (API)



Simple model (sync)



Threat intelligence sharing in GridPP

- Use WLCG MISP as focus
  - **Register (CERN account and/or Federated Identity)**
  - **Remotely access data on misp.cern.ch**
  - **Discuss sharing with Campus Security Teams**
  - Test API to pull data locally
  - Test Web app (+sync)
  - Integration with security tools (Bro)

Conclusions

- Progress made in developing expertise in Bro and MISP

- Clear area where GridPP can contribute as a community

- Not quite done…

Stop Press!

- SOC WG Workshop/Hackathon
  - Help attendees with deployment of security tools like Bro and MISP at their local sites
  - Where possible anticipate sites having resources identified prior to workshop to allow for assisted deployments
  - Looking at December time frame to allow for site preparations, co-located with pre-GDB
  - Anticipated to take place at CERN
  - Inform next steps for working group
  - Talk to me later!