CERN’S SECURITY OPERATIONS CENTRE

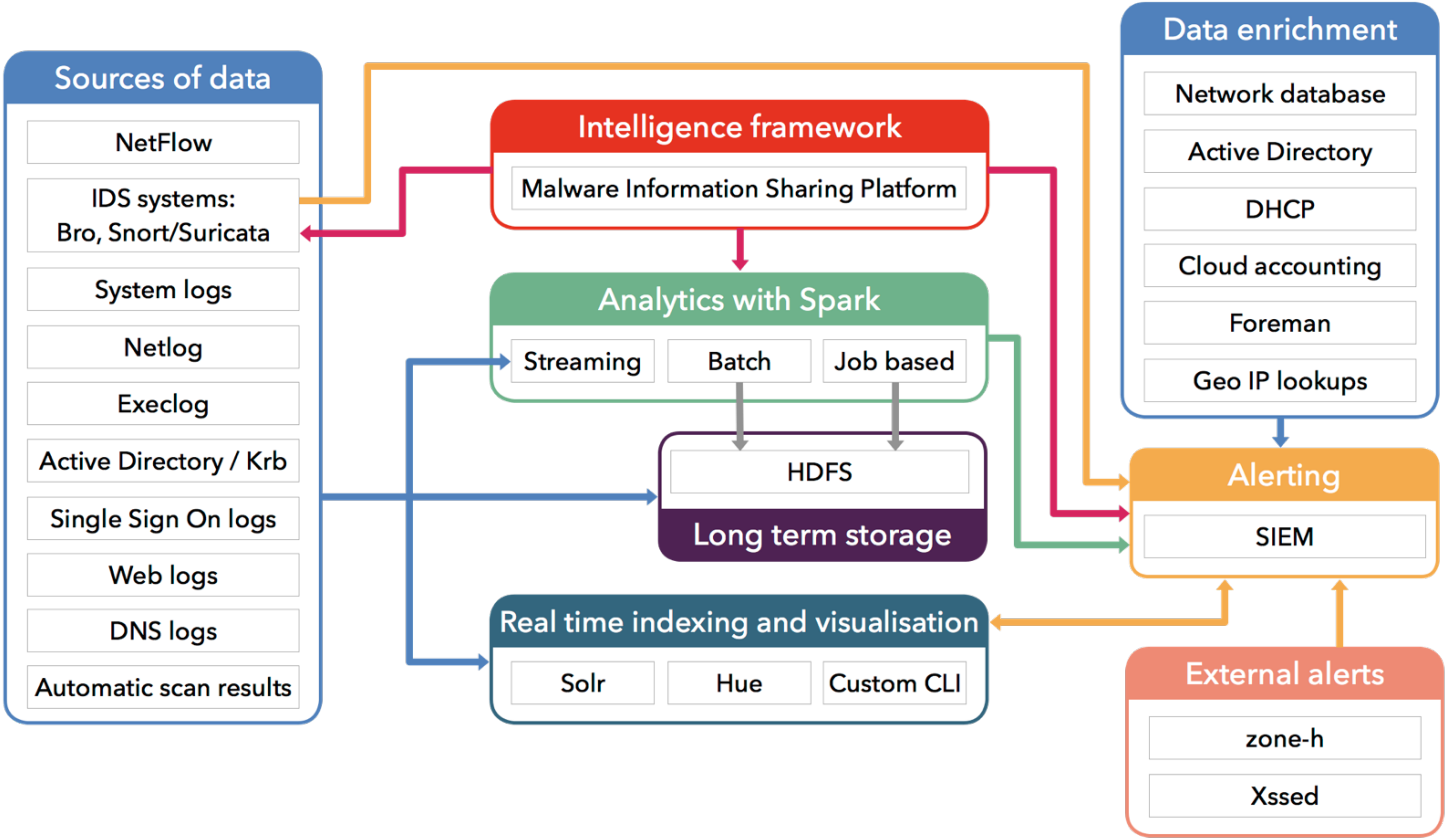
GDB, 7TH OF MARCH 2016

LIVIU VÂLSAN

The CERN SOC

- Unified platform for data:
  - Ingest
  - Storage
  - Analytics
- Multiple data access / view patterns
  - Command line interface
  - Web based dynamic dashboards for querying and reporting
- Extensible, pluggable, modular architecture
- Data access control policies enforced throughout the system

Architecture of CERN’s SOC



Sources of data
- NetFlow
- IDS systems: Bro, Snort/Suricata
- System logs
- Netlog
- Execlog
- Active Directory / Krb
- Single Sign On logs
- Web logs
- DNS logs
- Automatic scan results

Intelligence framework
- Malware Information Sharing Platform

Analytics with Spark
- Streaming
- Batch
- Job based

HDFS

Long term storage

Real time indexing and visualisation
- Solr
- Hue
- Custom CLI

Data enrichment
- Network database
- Active Directory
- DHCP
- Cloud accounting
- Foreman
- Geo IP lookups

Alerting
- SIEM

External alerts
- zone-h
- Xssed

Achieving network level traceability with Bro

- Comprehensive logging of activity for offline analysis and forensics
- Port-independent analysis of application-layer protocols
- Support for many application-layer protocols including: DNS, FTP, HTTP, IRC, SMTP, SSH, SSL
- Analysis of file content exchanged over application-layer protocols, including MD5/SHA1 computation for fingerprinting
- Real-time integration of external input into analyses
- Support for IDS-style pattern matching
- Event-based programming model

Threat Intelligence Management at CERN

- After having evaluated both CIF and MISP, we've deployed and started using MISP at CERN
- Currently participating in multiple threat intelligence sharing projects:
  - > 2700 security events, with > 145000 IoCs, from > 90 organisations in the CERN SOC
  - All IoCs currently being fed to the Bro IDS, streaming analysis next
- We can help setting up a WLCG MISP infrastructure
  - Need to agree on conventions for information sharing
  - Put emphasise on the creation and sharing of high quality IoCs, avoiding duplication of data

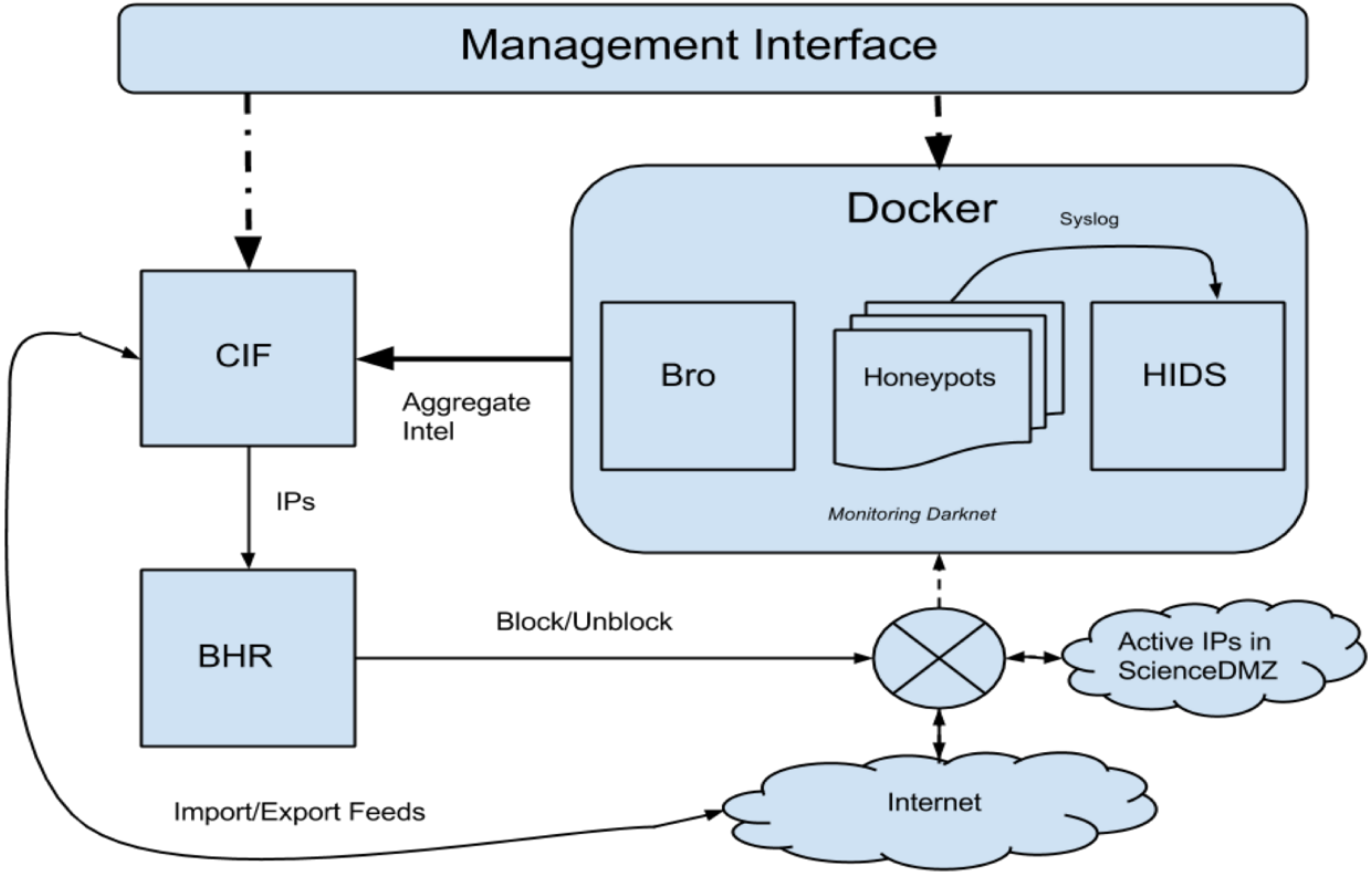
Current status of the CERN SOC

- Design finalised
- Development ongoing on the different modules
  - PoCs tested for each of the modules
  - Working on integration
  - Scalability testing
  - Adding more sources of data as we scale out
- In the future we should be able to accommodate VOs on our SOC
  - It would be good to know what amount of data we can expect
  - Take a gradual approach

How about a SOC appliance for sites lacking expertise?

- Designing a fully fledged SOC requires a lot of experience and effort
- We can provide full documentation of our SOC design and implementation for sites interesting
- Having a security appliance for sites is not a new idea
  - The National Science Foundation is founding a project to develop a Science DMZ Actionable Intelligence Appliance
  - Could a similar kind of appliance be used for WLCG sites, providing partial ?

Science DMZ Actionable Intelligence Appliance


Management Interface
Docker
Syslog
CIF
Bro
Honeypots
HIDS
Aggregate Intel
Monitoring Darknet
IPs
BHR
Block/Unblock
Active IPs in ScienceDMZ
Internet
Import/Export Feeds