SOC Working Group Workshop/Hackathon

David Crooks and Liviu Vâlsan

david.crooks@cern.ch

liviu.valsan@cern.ch

GDB, November 2017

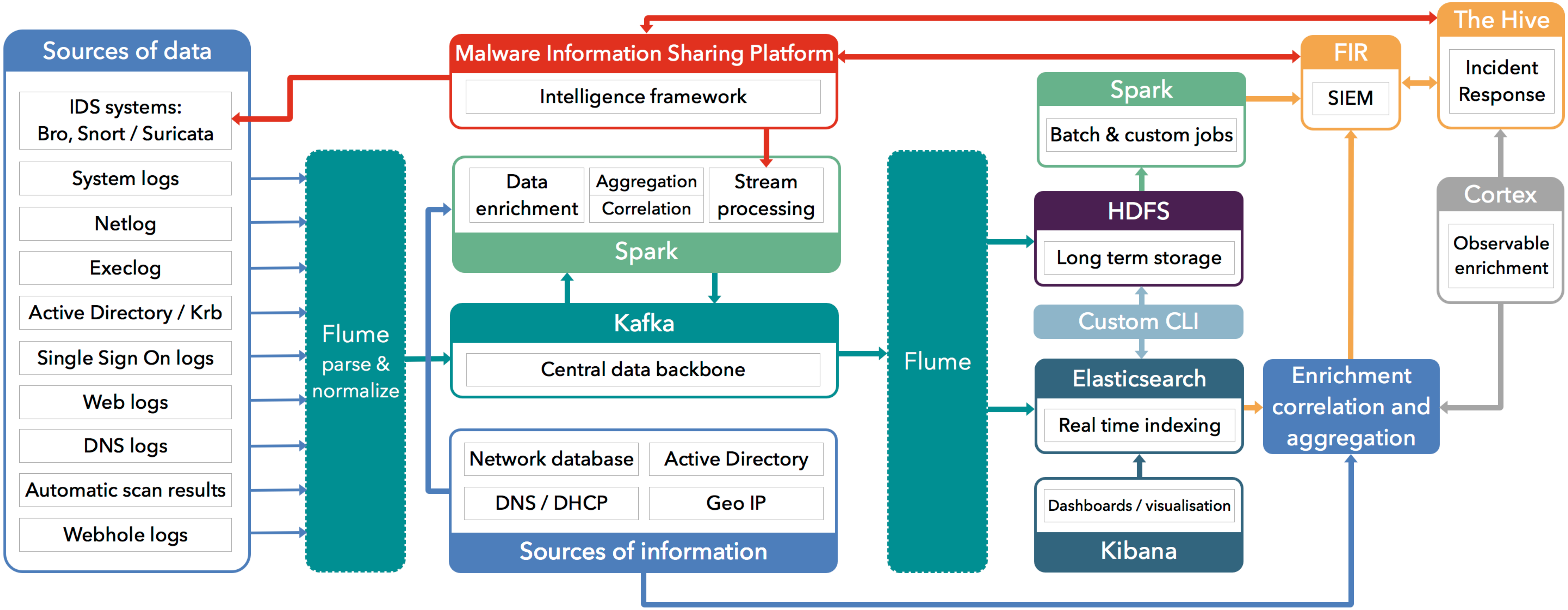
WLCG
Worldwide LHC Computing Grid

Security Operations Centers

- Apply analytics concepts to security platforms

- *Create a scalable reference design applicable for a range of sites by examining current and prospective SOC projects & tools.*

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
Spark
Batch & custom jobs
HDFS
Long term storage
Custom CLI
Elasticsearch
Real time indexing
Dashboards / visualisation
Kibana
FIR
SIEM
The Hive
Incident Response
Cortex
Observable enrichment
Enrichment correlation and aggregation

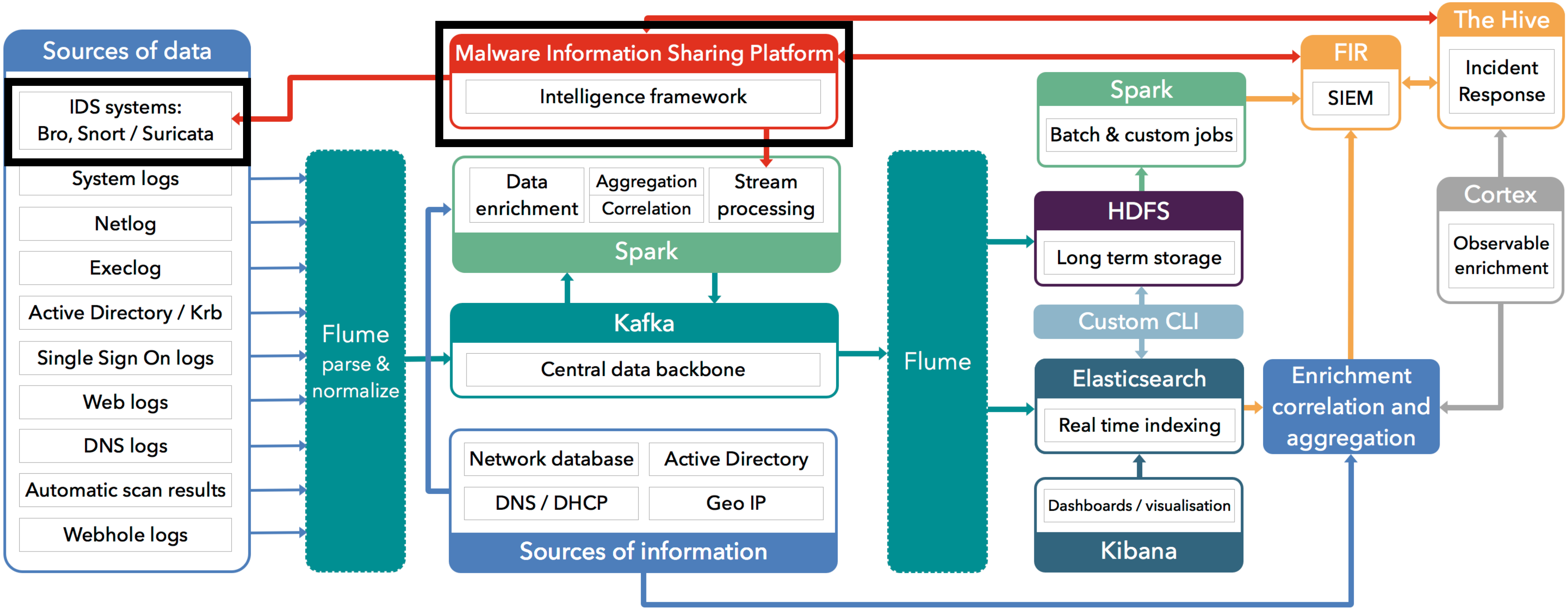
CERN SOC

- 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)

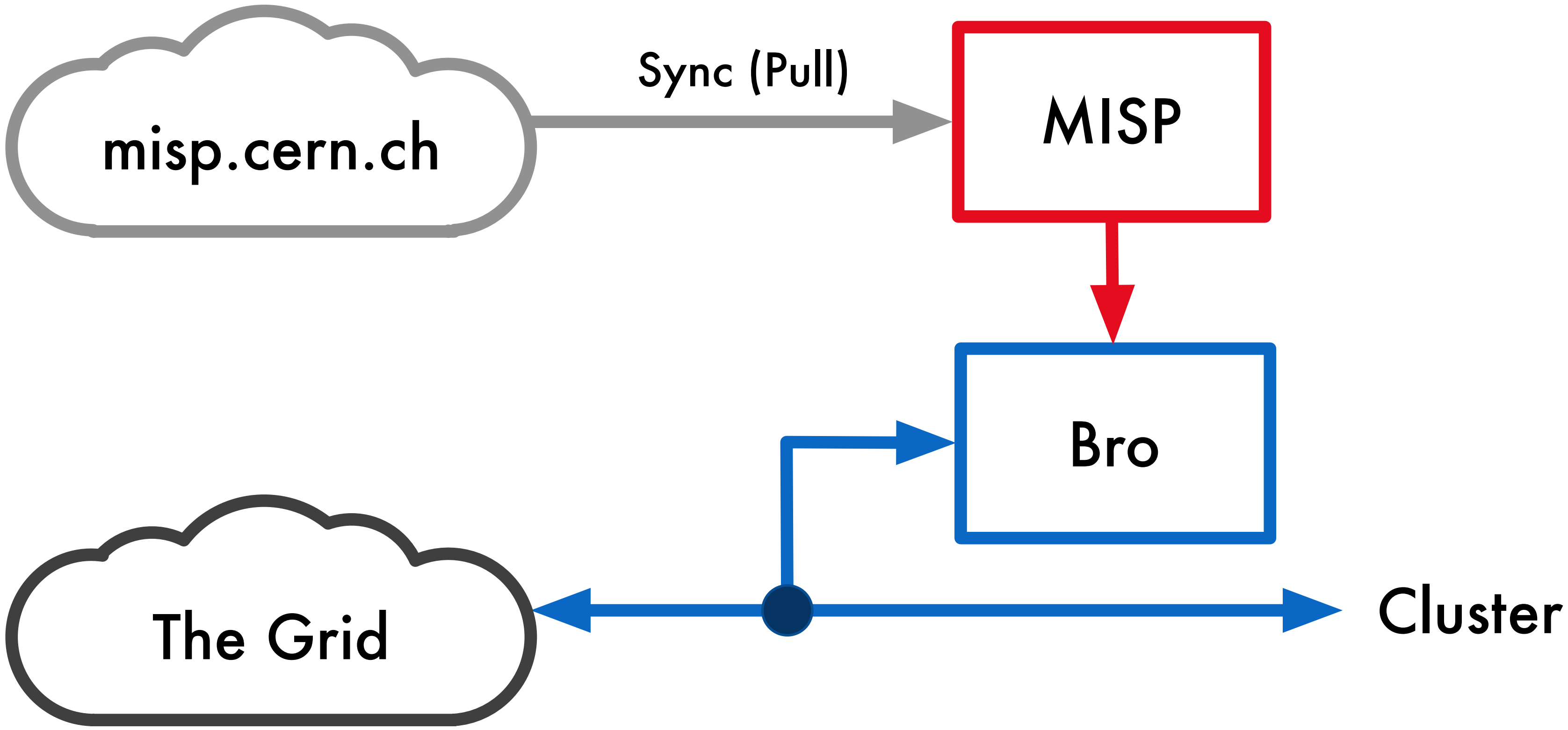
Technologies

- Look for minimum viable product
- Intrusion Detection System (IDS)
  - Bro
- Threat Intelligence
  - Malware Information Sharing Platform (MISP)

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
Spark
Batch & custom jobs
HDFS
Long term storage
Custom CLI
Elasticsearch
Real time indexing
Dashboards / visualisation
Kibana
FIR
SIEM
The Hive
Incident Response
Cortex
Observable enrichment
Enrichment correlation and aggregation

Simple model (sync)



Workshop/Hackathon

- Taking place at CERN over 11th and 12th of December
- Format will be that of a hands-on hackathon
    - Aim to 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

Areas of focus

1) Installation of Bro

2) Installation of MISP

3) Integration of Bro & MISP

4) Enrichment of Bro data and integration into wider SOC components

Agenda

Monday 11th December 2pm-6pm

- Introduction
- Demonstration of CERN SOC
- Discussion of outcomes for the workshop including necessary components and specific goals of individual sites

Agenda

Tuesday 12th December 9am-6pm

- Guided workshop
- Identify areas where sites can work together, for example to generate provisioning modules or to enhance existing documentation
- Wrap up period to include feedback, ongoing activities generated from workshop, future goals for working group, and potential future workshop plans

Guide timeline (Tuesday)

9-10: Initial site preparation including network and basic configuration

10-12: Initial installation and configuration of Bro

2-3: Initial installation and configuration of MISP web instance

3-4: Integration of MISP and Bro

4-6: Discussion

More details…

- Register (in person or remote attendance)
  - https://indico.cern.ch/event/676160/
- More information
  - https://wlcg-soc-wg.web.cern.ch/
- Contact
  - David Crooks (*david.crooks@glasgow.ac.uk*)
  - Liviu Vâlsan (*liviu.valsan@cern.ch*)