WLCG SOC Working Group

David Crooks
david.crooks@cern.ch

Liviu Vâlsan
liviu.valsan@cern.ch

ISGC March 2018

WLCG
Worldwide LHC Computing Grid

Introduction

- Following on from ISGC 2017
  - WLCG Security Operations Centres Working Group
- Security Operations Centres Working Group created in 2016
  - Requirement to monitor new virtualised cluster environments, including those using containerisation
  - Potentially more opaque than existing grid systems
  - Network monitoring key to understanding cluster state

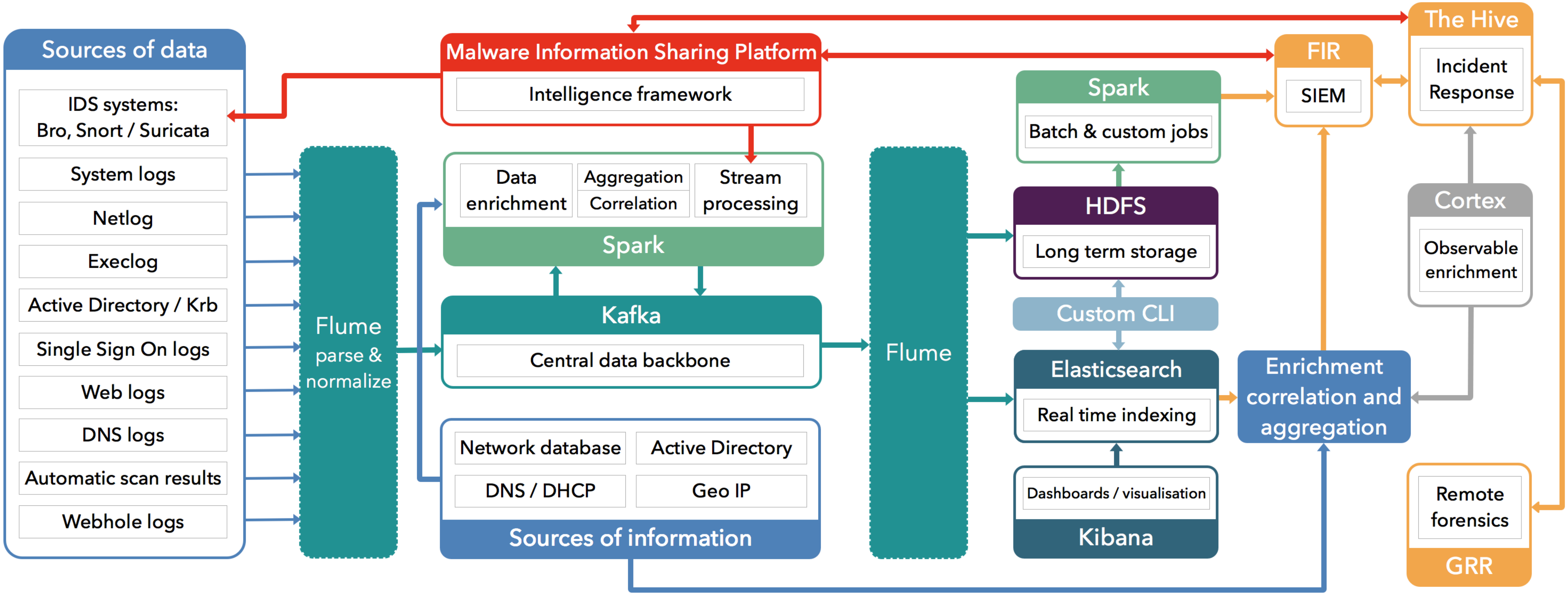
Security Operations Centre

- The purpose of a Security Operations Centre (SOC):
  - Gather relevant security monitoring data from different sources
  - Aggregate, enrich and analyse that data for use in the detection of security events and any subsequent actions
- A SOC consists of a set of software tools and connective processes

Mandate

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

CERN SOC



See **Building a large scale Intrusion Detection System using Big Data technologies**, Thursday 2pm

Framing questions

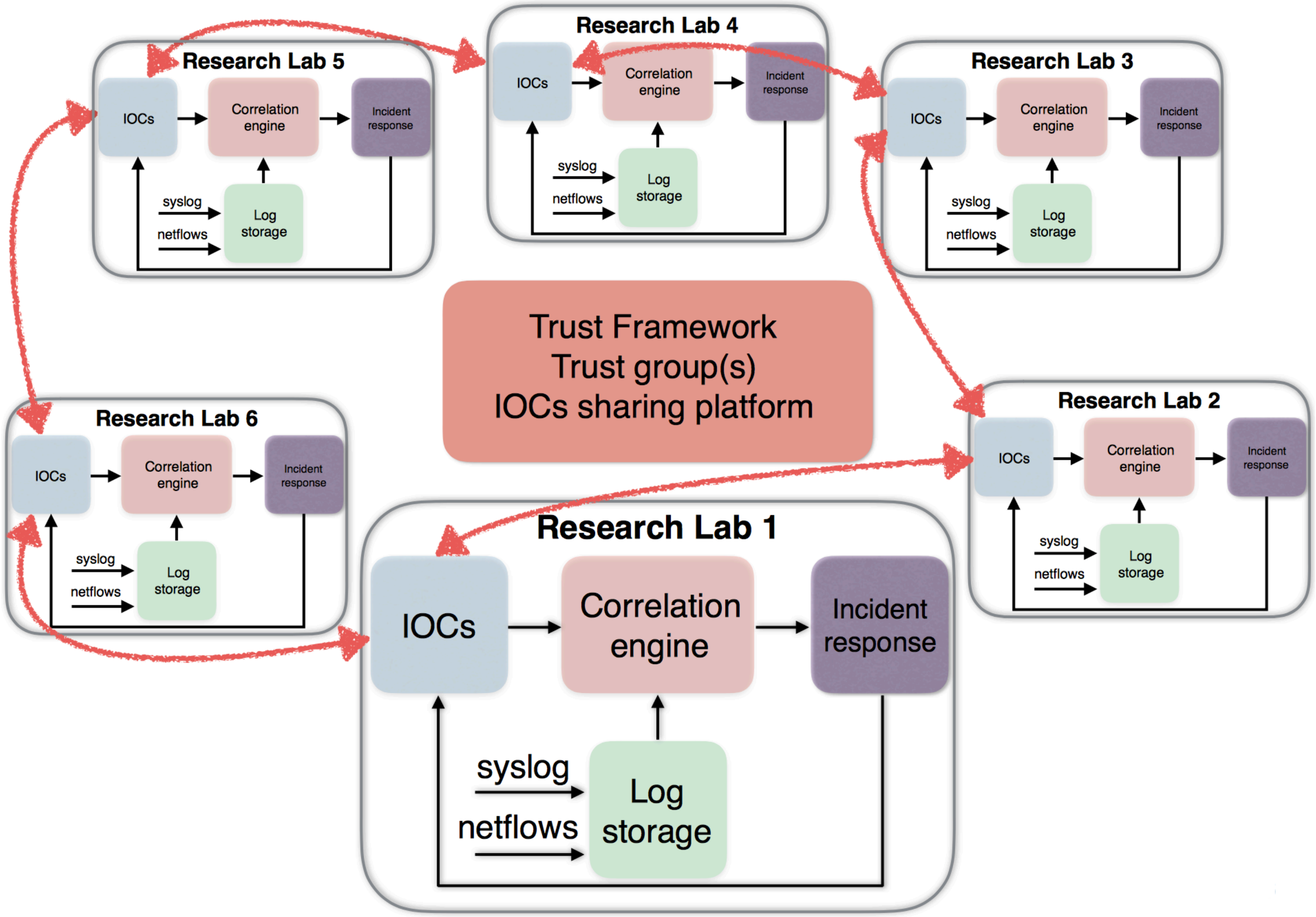
- What is happening inside my cluster and network?
- What information do I have on (external) events?

- Build out a reference SOC from basic components

Network Monitoring

- IDS: Bro [www.bro.org]
- Wide use in the US
  - 100 Gbps setup at Berkeley Lab
- Flexible & Scalable
  - Comprehensive logging of network activity
  - Deep packet inspection up to application-layer protocols
  - Analysis of file content, including MD5 / SHA1
  - Integration of external Indicators of Compromise

Threat Intelligence



- The future of academic computing security

  - CHEP 2016 (Romain)

IOC: Indicator of Compromise

Threat Intelligence

- Common response + shared responsibility
- Fundamentally collaborative
- Malware Information Sharing Platform [www.misp-project.org]
- Facilitates development of trust frameworks between sites to allow rapid sharing of threat intelligence

Two strands

- Technology stack
  - Technology needed to build a SOC
  - (starting from) Bro + MISP
- Social/cultural:
  - Social and cultural shift in sharing of intelligence
    - One goal of this group is to explore collaboration between grid and institute / campus security teams
    - Threat intelligence + collaboration

December Workshop 2017

- First SOC WG Workshop/Hackathon took place late 2017
- Deploy two core components of reference SOC model (MISP + Bro)
- Integrate MISP and Bro
- Provide access to documentation
    - Encourage sites to contribute back with their configurations
- 27 registered attendees from 19 institutes in 8 countries
    - Over half in person, with most for both days

MISP

- Deploy MISP
  - All sites able to deploy MISP after work with provisioning systems
  - CERN Puppet modules used as reference (masterless + server/client)
- Sync events from WLCG MISP instance [misp.cern.ch]
  - Most new instances configured syncing with WLCG instance
  - Some ongoing work to resolve remaining specific configuration

MISP

- How could we share threat intelligence in our community?
    - Addressed at WLCG / NGI / Institution level

WLCG	Central MISP instance hosted at CERN
NGI	UK
Institution	IN2P3 [France] University of Glasgow [UK]

MISP

- Next steps
  - Access to WLCG instance is primarily via eduGAIN+SIRTFI enabled institutional Identity Provider
  - Preparation for the future: if a site's institution is in eduGAIN but not SIRTFI enabled, they should talk to their Identity Provider
    - https://refeds.org/sirtfi

Bro

- Discuss network taps / locations
    - Discussed CERN configuration and different possible approaches
- Deploy Bro
    - Several sites have Bro deployed
        - At least seeing workers running / logs generated

Bro

- Next steps
  - Continue deployment of Bro
  - Tuning (sample rates, network configuration)
  - Plan to increase monitored network traffic as experience gained

MISP and Bro integration

- Script to generate Bro import data from MISP IOCs
  - Tested pulling data from MISP to Bro instances using MISP API
- Next steps
  - Complete import into Bro

Summer workshop

- Following success of December workshop, currently planning next iteration
- Current plans
  - Expanded length to 2.5 days
  - Located in CERN
  - Expanded agenda based on morning/afternoon sessions (see next slide)
  - Deciding on dates - last week of June/first week of July
    - Finalise dates to announce at WLCG/HSF Workshop [foodl poll]

Summer workshop agenda

- Initial steps
  - Simplified version of December workshop capitalising on new documentation
- Network topology
  - Closer look at possible network tap points and strategies
- Elasticsearch and associated tools
  - Visualisation
- Advanced aggregation, correlation and enrichment of generated alerts
  - Adding capabilities

Ongoing questions

- What (sources of) data do we need (intersection with traceability)
- How to handle data sharing + protection for different user groups
- How to consider different contexts: Institution / NGI / WLCG / Other
- New framing question
  - When a security incident is detected how can we get the full picture of the incident?
    - When exactly it started, what is the extent of the incident…

Conclusions + next steps

- Steady progress in adding new contributors
- Adding sites with MISP experience
- Gaining general experience with Bro
- Focus on key areas of work
- Workshop shown to be useful forum for this work

Group contact details

- Website
  - wlcg-soc-wg.web.cern.ch
- Mailing list
  - wlcg-soc-wg@cern.ch
- Documentation
  - wlcg-soc-wg-doc.web.cern.ch