Security update

Vincent Brillault, Hannah Short, ***Liviu Valsan, Romain Wartel***

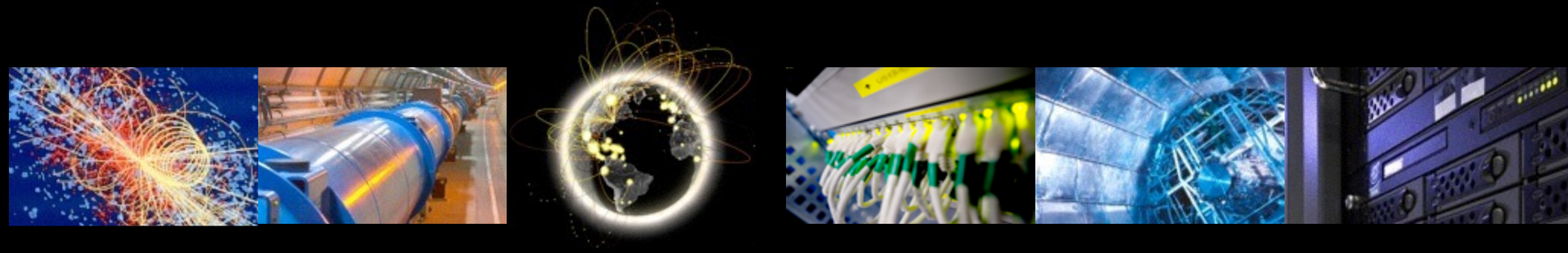
WLCG Workshop 2017, Manchester, June 19-22, 2017

WLCG
Worldwide LHC Computing Grid


gLExec

Singularity & Security

Traceability & isolation



WLCG
Worldwide LHC Computing Grid

From gLExec to Singularity?

- gLExec: User traceability and isolation
  - User authenticated through X.509 proxies
  - Remote calls for audit and ACLs (suspension)

- Singularity: Pure isolation solution
  - No traceability provided, no remote call to Argus
  - End-user authentication (X.509 proxy) not required
    - Can still be needed for e.g. storage access
      - But maybe we can evolve to do without / differently?

How to maintain traceability?

- Trust the VO framework & pilot jobs
  - If Singularity is properly used, pilot is protected from user payload
  - VO infrastructure already used for operational issues
- Ask VO to provide user traceability
  - Results of first basic challenges encouraging
  - Challenges should be ran regularly
- Traceability still possible at site (if needed)
  - VO pilot could send user session start / end
  - User identifiable by artefacts in running jobs

Long term support

- Isolation without SUID (unprivileged user namespaces) could come part of the OS as early as RHEL 7.4
  - All security parts handled by the kernel
  - Security issues handled by Red Hat
  - *New* technology, could mean more critical kernel vulnerabilities

No remote call: ACLs / suspension?

- Singularity doesn't remotely call Argus
  - No central emergency suspension through Argus
  - User emergency suspension still possible through VOs

- ACLs / suspension still needed at sites:
  - For submitting jobs
    - Could be simpler if no local submission: only pilot jobs?
  - For storage?
    - Non proxy-based authentication already used by e.g. Alice

- Long term requirement for Argus at sites?

Authorization working group

- Upcoming environmental changes impact our authorization system:
  - New General Data Protection Regulation
  - Identify federation
  - Singularity, Argus, etc.
  - OSG started to use COmanage

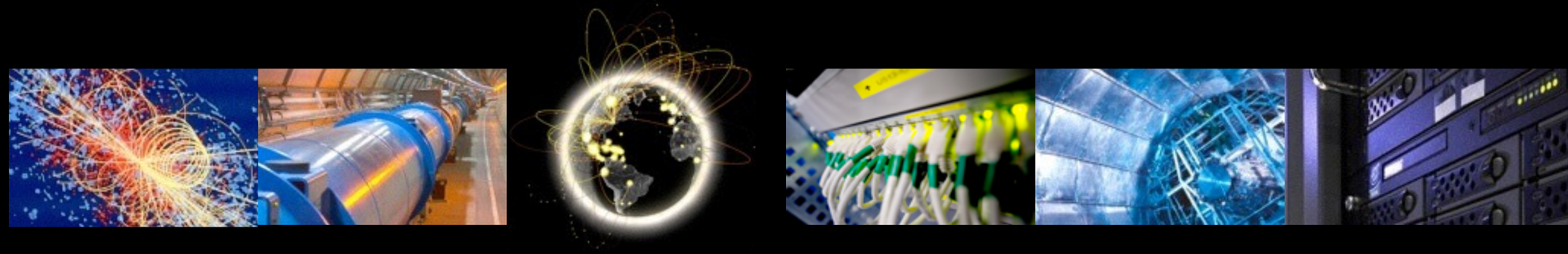
Authorization working group

- Creation of a new time-limited WLCG working group on authorization
  - Review the current status and technologies
  - Evaluate the needs of the WLCG VOs and sites for the coming years
  - Assess impact of expected changes above
  - Make recommendations on the next steps (strategy, architecture, technologies)
  - Regular reports in the GDB
  - Open group: anyone interested invited!
    - In particular, crucial to involve OSG, VOMS and Argus maintainers!

WLCG Personal Data Protection Policy

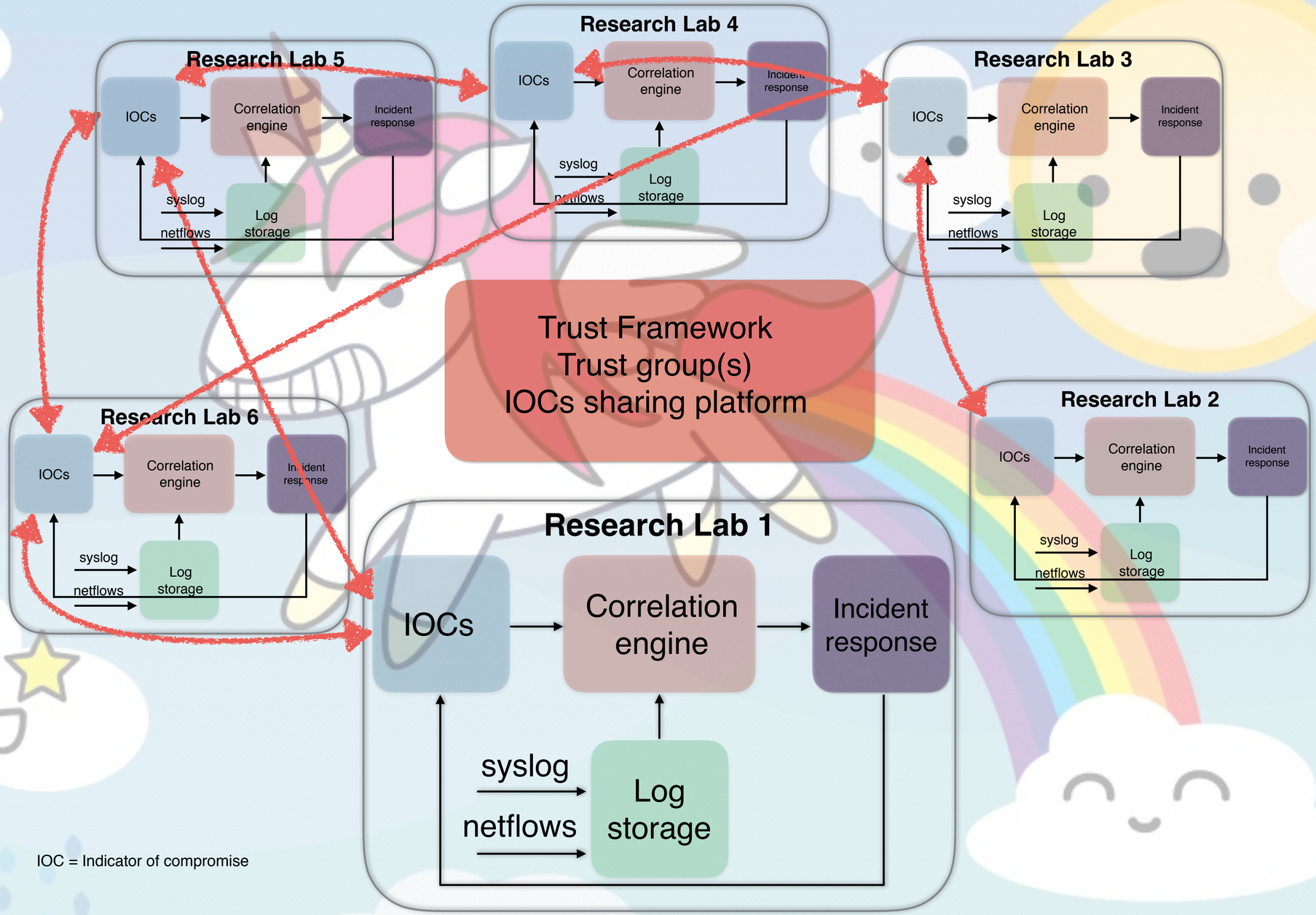
- New WLCG DPP available at
  - https://documents.egi.eu/document/2732
- Triggered by the EU General Data Protection Regulation (GDPR)
  - Will come in effect May 25th 2018
- What are the implications for VOs?
  - Need to review needs & requirements on usage of Personal Data
  - Prepare a “Privacy Policy” for end user on all service entry points
    - Template available

Collaboration with, and between, security teams

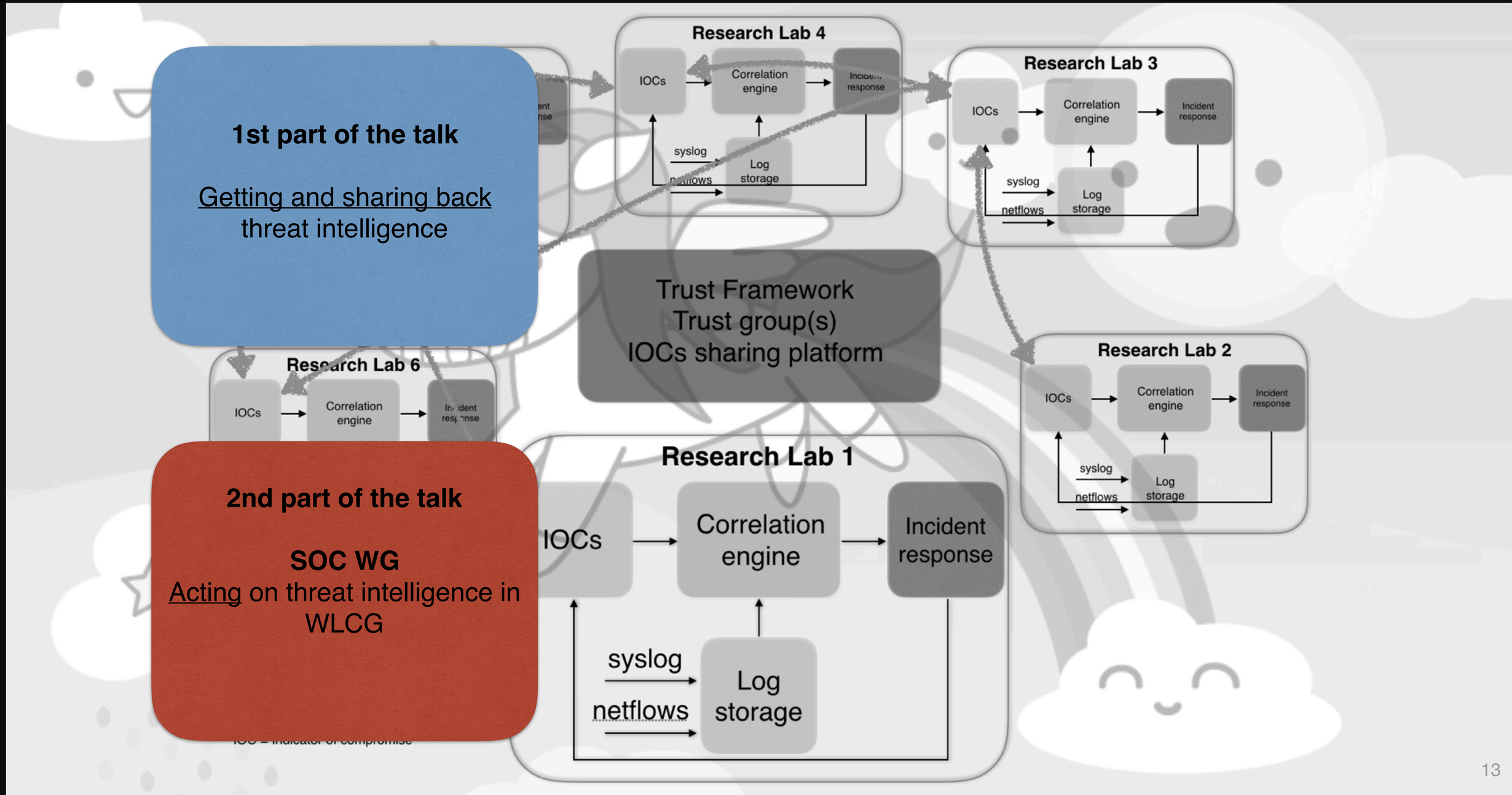


WLCG
Worldwide LHC Computing Grid

Conclusion from the last WLCG workshop



This talk


1st part of the talk
Getting and sharing back threat intelligence
2nd part of the talk
SOC WG
Acting on threat intelligence in WLCG
Trust Framework
Trust group(s)
IOCs sharing platform
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
Research Lab 2
IOCs
Correlation engine
Incident response
syslog
netflows
Log storage
Research Lab 1
IOCs
Correlation engine
Incident response
syslog
netflows
Log storage

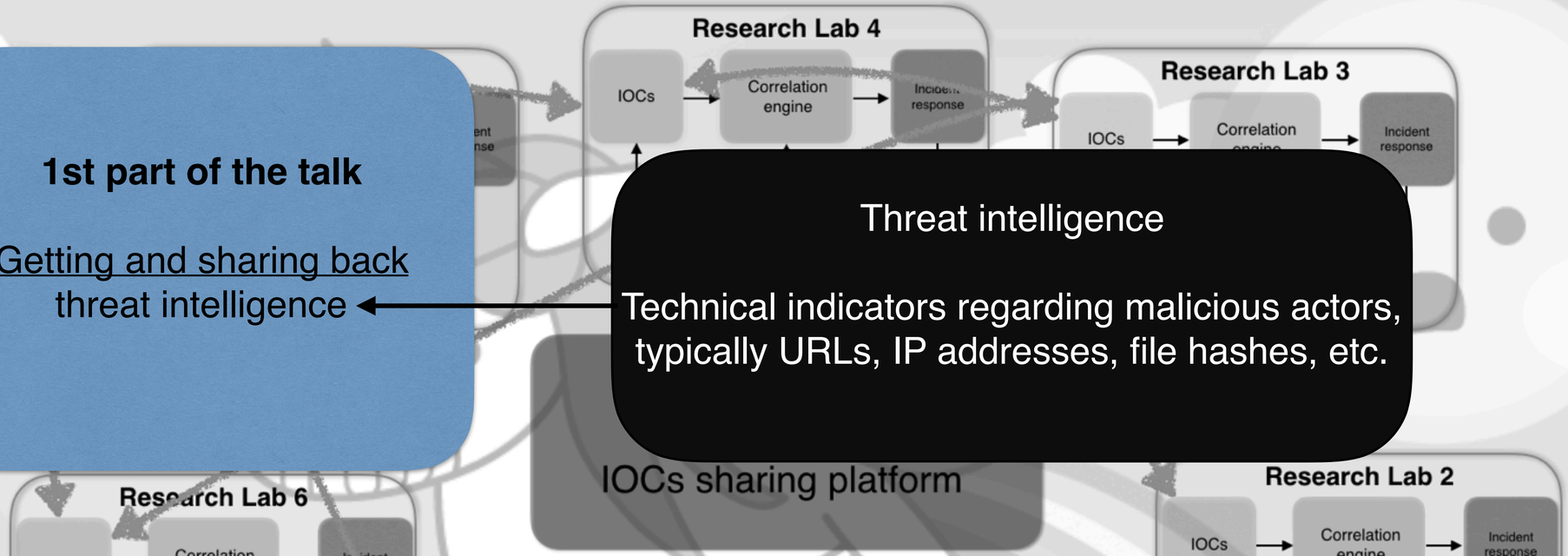
This talk

1st part of the talk

Getting and sharing back threat intelligence

Threat intelligence

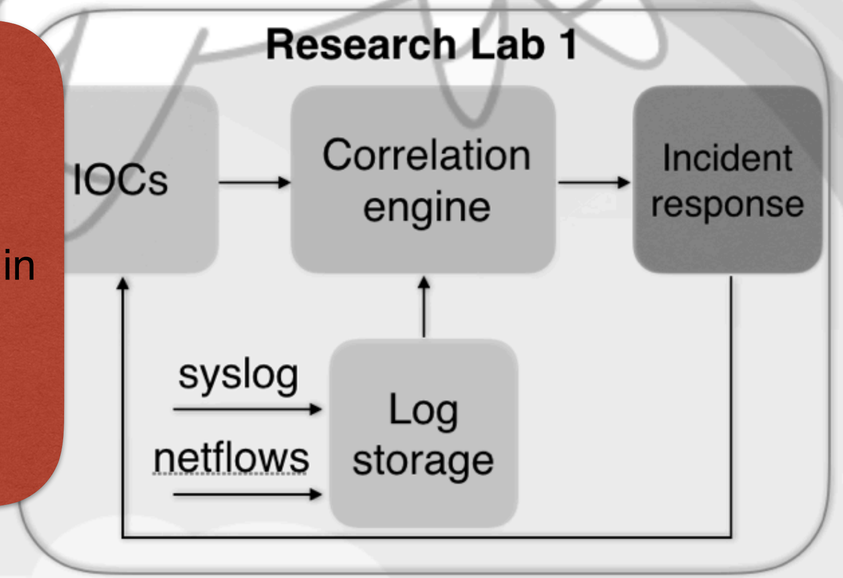
Technical indicators regarding malicious actors, typically URLs, IP addresses, file hashes, etc.



2nd part of the talk

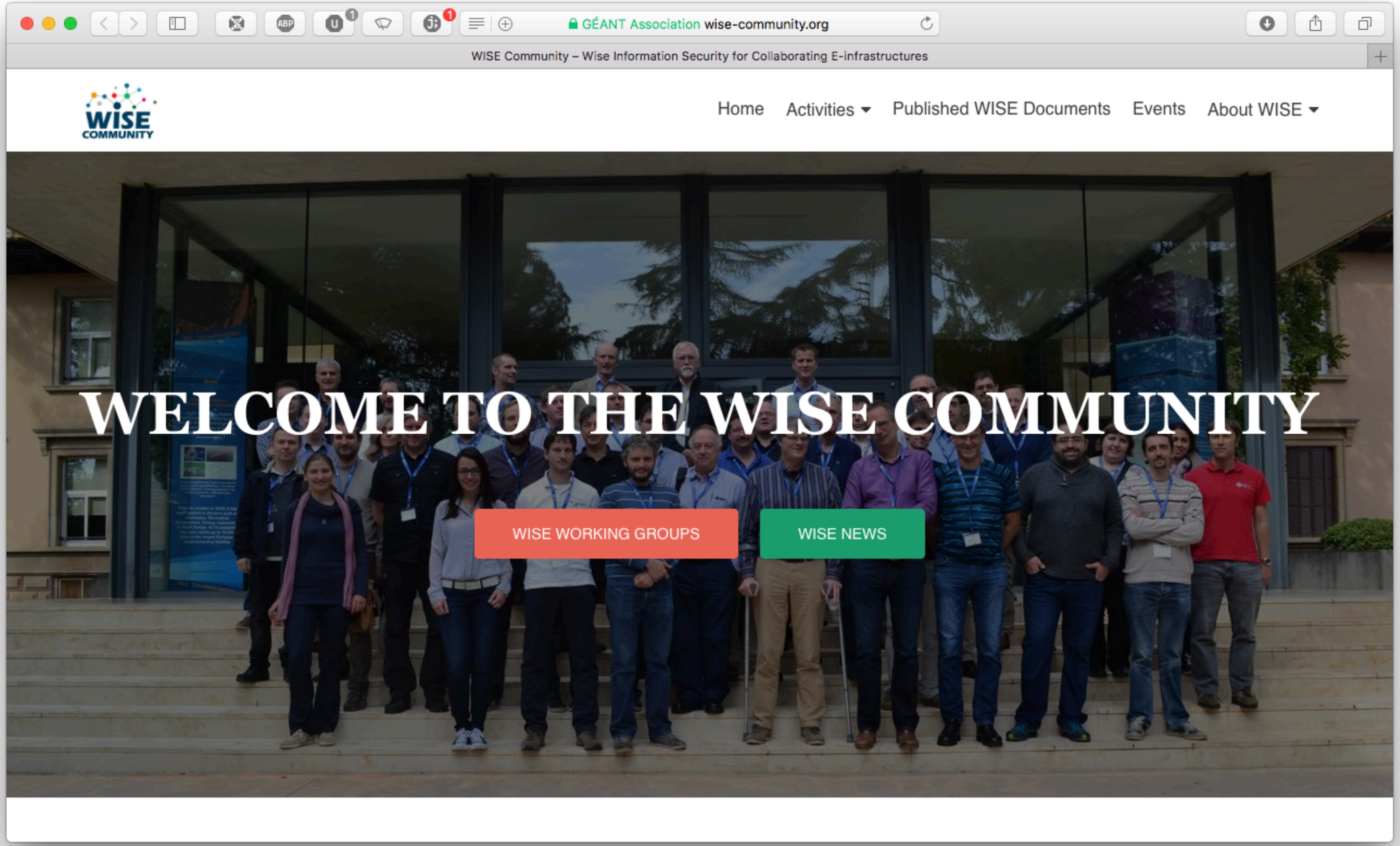
SOC WG

Acting on threat intelligence in WLCG



IOC = Indicator of compromise

WISE Information Security for Collaborating E-infrastructures



Threat intelligence sharing

XSEDE Extreme Science and Engineering Discovery Environment

PRACE

EUDAT

GÉANT

CERN

Open Science Grid

LSC LIGO Scientific Collaboration

EGI

WLCG Worldwide LHC Computing Grid

Human Brain Project

NCSA

Project-based sharing

Membership based on **affiliation**

?

Adhoc sharing

Membership based **peer vetting**

Newcomer: China

中国科学院
CHINESE ACADEMY OF SCIENCES

- China Cyber Security Federation for High Energy Physics
  - "Chinese security federation"
  - Federation of Chinese institutes / universities / CAS
- Just getting started
  - WLCG and others will actively support the Chinese security federation
  - Crucial for HEP security operations
  - Valuable contacts and connections for other communities too
- Security Workshop 9-13 October 2017

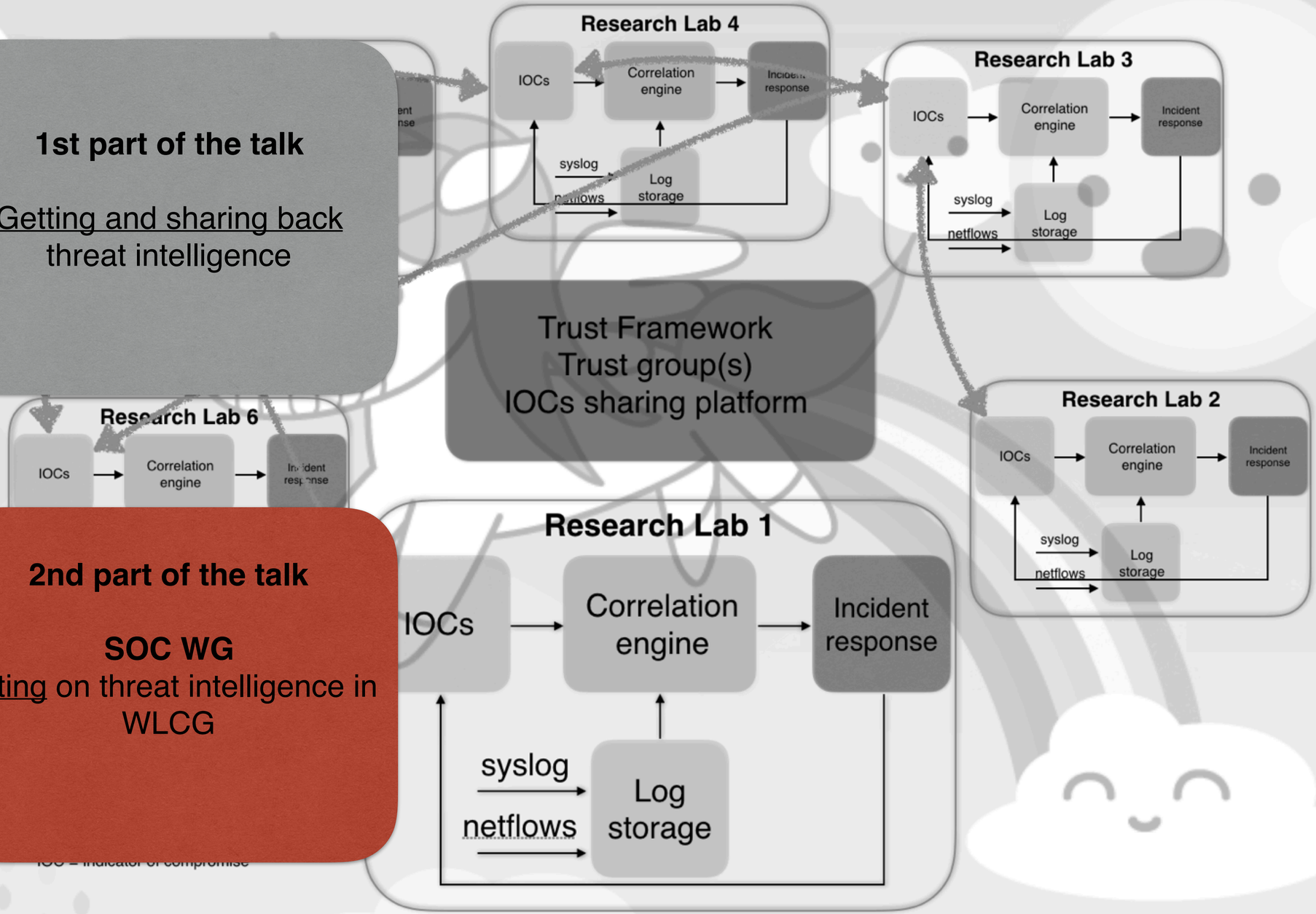
This talk

1st part of the talk

<u>Getting and sharing back</u>
threat intelligence

2nd part of the talk

SOC WG
<u>Acting</u> on threat intelligence in WLCG



WLCG SOC Working Group

- A Security Operations Center (SOC) is a centralised system dealing with the detection, containment and remediation of IT threats.

- WLCG Security Operations Centers Working Group mandated to:
  - Create a scalable reference design applicable for a range of sites by examining current and prospective SOC projects & tools.
  - Establish a clear set of desired data outputs and necessary inputs.

WLCG SOC WG Ongoing Activities

- Minimal viable product:
  - MISP (threat intelligence)
    - Deployed central MISP WLCG instance; instances at a number of sites
  - Bro IDS (intrusion detection and alerting)
    - Deployed at CERN and at number of sites
    - Different network topologies, usage metrics being gathered
- Examine Metron as a reference framework

WLCG SOC WG Call for Participation

- Deployment of Bro and testing of integration with MISP
  - Using central WLCG MISP instance or local instance
- Validating various network setups and ways of tapping into the network traffic using Bro
- Collection of Bro logs and processing of alerts using tools / frameworks already available at the site (ELK for example)

Details and how to join?

- Website: https://wlcg-soc-wg.web.cern.ch
- Indico category for meetings
- E-group: wlcg-soc-wg
- Mailing list: wlcg-soc-wg@cern.ch