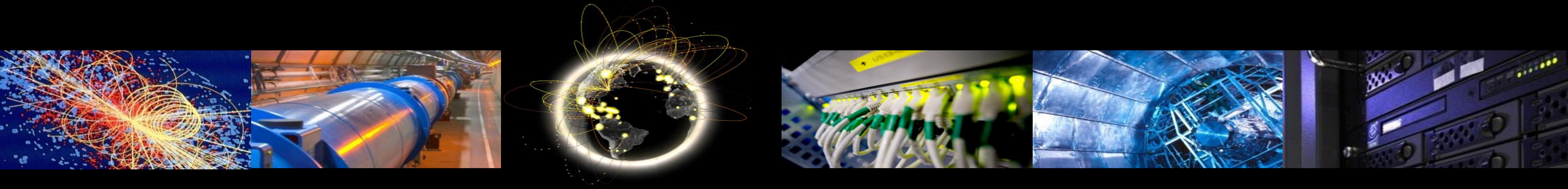
Traceability Update

Vincent BRILLAULT, CERN/EGI-CSIRT

GDB, December 2019



Traceability/Isolation WG update

- Working group proposal approved by WLCG MG
- Discussed at the last SPG meeting (early October)
  - Not adding a new policy, redesigning existing ones
- VOs expected to implement the recommendations
  - Final policies/requirements not expected to diverge
  - VOs contacted for update, no response so far…

Recent examples of traceability exercises

- EGI SSC-19 identified multiple issues:
  - Missing procedures within the VO, wrong contacts
  - Logs not kept for long enough by the VO
  - Sites not knowing how to investigate malicious jobs
- EGI-OSG coordination exercise confirmed it:
  - Not able to identify malicious jobs at sites & at the VO

Going Forward: More challenges

- Initial self-assessment from WG not enough
  - Didn’t identify issues found in more concrete exercises

- EGI SSC: too much effort , too focused for this?
  - Focusing on all sites of a single VO, not on all VOs
  - Long to setup up, heavy to run for sites, CSIRT & organizers

- A new simpler challenge: one malicious job for each VO?
  - Only ensuring that VO traceability is really in place

Going Forward: Forensic documentation

- EGI forensic documentation focused on compromised servers
  - Not really covering malicious jobs investigations
- Proposal: EGI to compile/coordinate new documentation
  - For each major job framework: what to look for & how (commands)
  - For each VO:
    - What can be extracted from pilot jobs? What helps the VO trace the job?
    - Where to look for? Files, paths, commands
- Help needed from experts in job framework and from VOs
  - Please contact me if you have knowledge to share

Summary (TL;DR)

- WG recommendations approved by WLCG MG
  - Implementation ongoing/pending

- New lightweight challenge needed for validation

- New forensic documentation coordinated by EGI