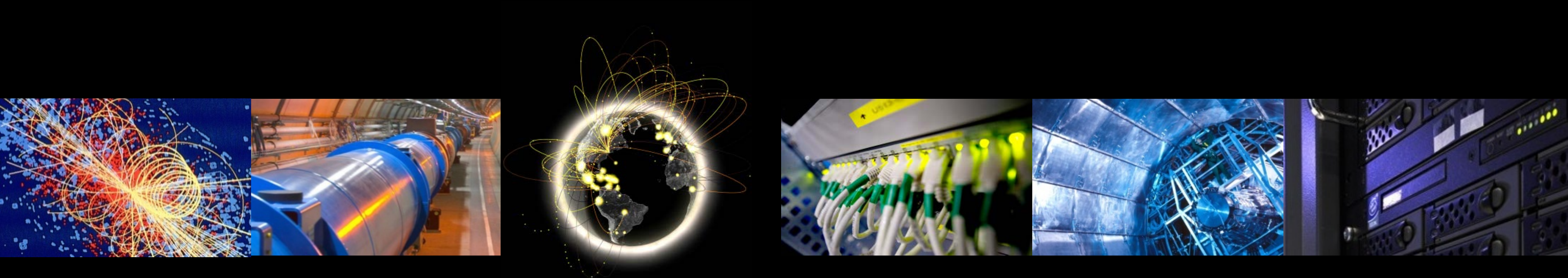
# Traceability & isolation evolution

Vincent BRILLAULT, CERN/EGI-CSIRT

GDB Mars 2015, Amsterdam



# Overview

- Why traceability and isolation ?
- Current situation
- What’s “new”
- “glExec”
- Black boxes
- The future?

# Why?

For security, but not only!

- Traceability: Identify, reconstruct & understand
  - Security incidents: catch bad users, fix vulnerability
  - Issues/bugs/strange behaviors

- Isolation:
  - Prevent credential theft & impersonalization
  - Prevent jobs from harming each-other

# Current situation

- Site responsible for (policy-wise):
  - Recording all activity: when, where, who, what
  - Securely and centrally store logs for months
  - Process logs upon CSIRT request during incidents

- Identifying and isolating users:
  - WN/pilot jobs: glExec (if/when deployed & used)
  - Endpoint/services: end-user x509 certificate/proxy

- Multi-site analysis difficult:
  - Broadcast warning/regex and wait/hope…
  - Rely on VO frameworks or central services

# What's "new"

- New technology on the rise:
  - Virtualization & VMs: black boxes managed by VOs
  - Cgroups/namespaces: new isolation solution?

- Multi-user pilot-jobs on the decline

- VOs have large frameworks & log activity

# “glExec”

- Promising technology: cgroup & namespaces

- Explore new solutions:
  - Identify what needs to be isolated from users, e.g:
    - Pilot job own credentials (if kept)
    - VO logging facilities & framework callback (if any)
  - See if new technology can cover out needs
  - Identify/resolve OS dependencies (EL7+ ?)

- Accept a split log “responsibility”
  - When/where → Who: Site + VO
  - When/where → What: Site & VO

We may be able to retire glExec and close this debate!

# Black boxes

- Pilot jobs/VMs becoming black boxes
  - – Site: Log externally observable behavior
  - – VOs: Log what happens inside

- Identify how to keep site expertise:
  - – Identify strange behaviors (e.g. Bitcoin mining)
  - – Debugging/problem resolution

- Keep response capability:
  - – User suspension:
    - Service/endpoints: OK (x509 certificates/proxy)
    - Shared resources (e.g. network): ??
  - – Properly integrate VOs in response procedures

# The future?

- New model possible:
  - Consider pilot jobs/VMs as black box
  - Build and trust central security VO logs
  - Concentrate on unprivileged isolation

→ There is a lot of questions, no clear solution yet

- VOs’ expertise needed:
  - Keep making sure pilot jobs are protected
  - How to take advantage of job frameworks
- Sites’ expertise needed:
  - What data/access/control is needed
  - What technology can be supported