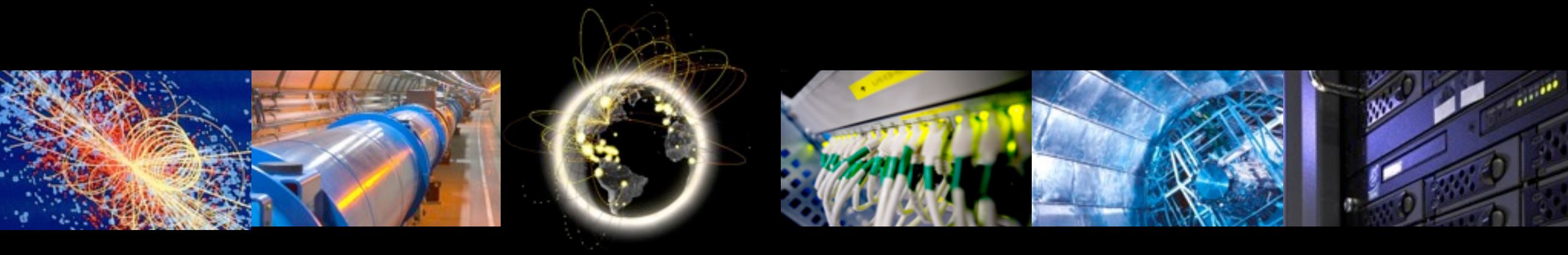
WLCG Group

WLCG Security

Romain Wartel

14th September 2010, EGI TF 2010, Amsterdam.



WLCG
Worldwide LHC Computing Grid

WLCG security

- WLCG security:
  - "Trust" relies on JSPG policies
  - Good collaboration between the EGI CSIRT, OSG and NDGF
  - LHC VOs involved sporadically
    - During security drills
    - During the recent security vulnerability campaigns

- Build on previous successes
  - Ensure coherent security strategies adopted by underlying grids
  - Ensure efficient information flow during security incidents
  - Ensure the LHC VOs are involved in security operations
  - Ensure trust between the WLCG participants
  - Avoid duplication of efforts

WLCG security officer

- WLCG Security Officer (~50% of an FTE)
  - This role addresses all issues of operational security
  - Main objective: coordination between the EGI CSIRT, OSG, NDGF security and LHC VOs
  - Coordinate the WLCG response to security threats against its infrastructure, which includes requiring actions from participants when needed, in particular in the context of serious vulnerabilities and security incidents;
  - Understand and assess the security risks faced by WLCG;
  - Advise and make recommendations to the project management, grid security teams and LHC VOs on security risks;
  - Contribute to the elaboration of security policies for WLCG participants and collaborate closely with the WLCG Security Policy Coordinator to ensure WLCG security policy issues are addressed.

Recent incidents

- The following incidents have been investigated in the last 6 months:

	Affects EGI	Affects OSG	Affects NDGF	Affects academic community
OSG-20100314		X		
EGI-20100722	X			
GRID-SEC-001	X	X	X	X
GRID-SEC-003	X	X		X

- Collaboration between grid infrastructures and also with the academic community is essential

Security incident coordination

- Response needs to be commensurate to the problem
  - Small incidents require little, localized effort
  - Large incidents require full-scale coordination
    - Several incident coordinators usually needed
    - "ad-hoc" organization of coordinators based on:
      - The localization and distribution of the compromises
      - The severity of the incident
    - GRID-SEC (http://cern.ch/grid-sec) for international incident response
  - Experiments also need to be more informed and involved
- Significant experience gained in the recent years
  - Collaboration between academic grids well established
  - Needs to continue!

WLCG security incidents management

- JSPG policies
  - Sites required to follow the incident response procedures
  - Security operations can also require actions from participants
- Main coordination tasks during security incidents
  - Manage the information flow
  - Ensure the relevant leads are followed: understand the cause
  - Technical work (forensics, help inexperienced sites, etc.)
- Multi-level coordination during security incidents
  - At the affected sites
  - Within each NGI
  - Within each grid infrastructure/project
  - Between different academic grids
  - With the involved external organizations

Handling security incidents

- When WLCG needs to deal with incidents, the priority is to:
  - Protect the project's reputation - our most valuable asset
    - Requires well established procedures and communication channels
    - Dealing with the media
  - Ensure service availability
  - Ensure data integrity
  - Limit the cost of security incidents
- Main causes of security incidents in the past year:
  - Compromised SSH passwords or keys at other sites
  - Vulnerable Web applications
  - Failure to apply security patches (root escalation)
  - Weak passwords or other local misconfiguration
- Our work plan needs to take this into account!