Security Parallel Session Summary

Ian Collier **David Crooks**

Joint WLCG & HSF Workshop 26-29 March 2018

Trust and policies

Policies and Trust

- 15 years of experience (WLCG policy started in 2003)
  - Building Trust in collaboration with others works best; forces us to produce general documents (of use to many); saves effort and improves quality
  - We will continue to work with others (EOSC, WISE, IGTF, TF-CSIRT, etc.)
- Ever-growing collaboration between Research Communities (shared IT resources)
- WLCG should not “go it alone”: Trust is as important as the technology and important that our AAI is interoperable and can easily co-exist with others

GDPR

- We are relying on the updated GEANT Code of Conduct to allow for data transfers outside of EU.
- Policy group will update the overall Data Protection Policy Framework and templates for services to write their Data Privacy statements.

Authentication and Authorisation: AuthZ WG

Objectives identified in last 6 months

- Gather requirements for a WLCG AAI to provide Membership Management & Token Translation services, to facilitate transition to token-based credentials

- Guide the development of AAI Pilot Projects: INDIGO IAM (pilot supported e.g. by EOSC-Pilot & AARC) and EGI Check-in & COmanage (pilot supported e.g. by AARC)

- Define a JSON Web Token (JWT) Identity and Capability Schema(s) and agree to its use among WLCG Participants

- Assess the AAI Pilot Projects against our requirements and move towards production deployment on a per-VO basis

Ongoing tasks

- Continue JWT Schema Definition; Guide development and testing of AAI Pilots; Assess overlap of WLCG AAI and CERN SSO Infrastructure

Operational Security

Risk landscape for the next 5 years

- Enable threat intelligence to be fully used by WLCG sites and convince site security teams to open up and collaborate

- Increase collaborations and build better trust relationships (globally and locally), and keep sites informed about malicious developments

Incident Response & Traceability

- First step towards potential joint EUDAT+EGI CSIRT: unify procedures, communication - AAI/Federated Identities: We probably need security policies & CSIRT?

- Traceability still possible with "black box" VMs/Pilot Jobs: External behaviour (sites) + user(s), payloads (VOs)

- Unprivileged containers are not simple yet!

Technology & Threat Intelligence

- We need collaborations and trust groups to share threat intelligence, the processes and culture in place to act on it, and the technology to enable this

- Discuss how to best progress work with campus trust groups and cultural change

Thank you to all speakers and attendees (local and remote)