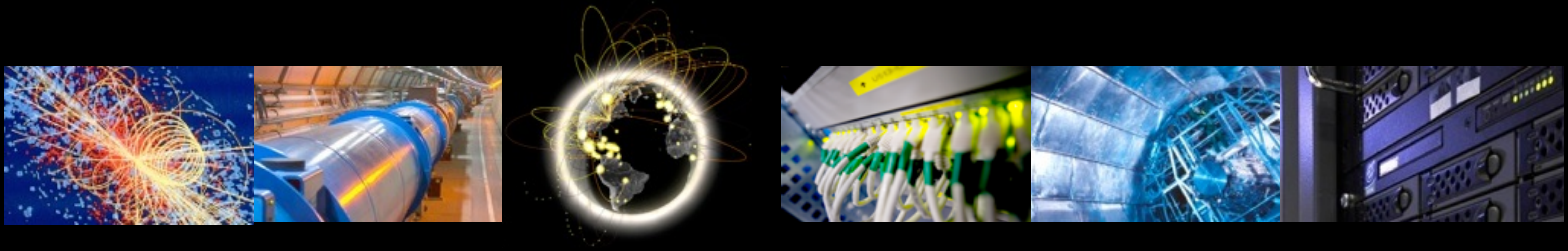
Addressing the OSG - EGI security cooperation issues



Romain Wartel

2019 Joint HSF/OSG/WLCG Workshop, 18-22 March 2019, JLAB

Collaboration is too weak

- OSG - EGI collaboration too limited on operational security issues
  - This is increasing risks for WLCG (and OSG/EGI)

- Sub-optimal points:
  - No shared security operations
  - No shared/common meeting, or regular calls
  - No cross-membership of team members
  - Common channel exists but is never used
  - Significant cultural gap, and expectations on the other side

Collaboration essential!

- Security landscape VERY different from 10 years ago
  - Start of LHC, SSH attacks, Linux Kernel rootkit etc.

- Our sites are the main target (and not “the grid”)
  - More rarely the infrastructure – Most abuse is cryptocurrency mining by insiders
  - International for-profit gangs target our sites
  - Foreign governments attack target our sites

- Academic and research institutions are valuable targets
  - They typically pay ransom
  - Great gateway to technologies – cheaper than attacking original manufacturer
  - Access to scientific data, R&D, journals very appreciated (by individuals or some nations)

- Our collaboration, reputation and funding are at stake

Collaboration essential!

- Our sites are the main target…

… And their best chance is a tight collaboration between security experts at the infrastructure/global level

- No site can defend alone against a foreign government or international gang
  1. Need to get connected to receive/share relevant threat intelligence
  2. Need technical means to respond (monitor traffic, correlate indicators, respond)

  – > WLCG, EGI and OSG security experts best placed to help achieve this

- Joining forces between OSG and EGI is very important
  - Same attackers, same malware, same users…
  - Yet limited resources, time, and expertise

Suggestions

- Different relationships with the sites and the Experiments/VOs
  - OSG works particularly closely with the Experiments
  - EGI works very closely with the sites
  - We have to take advantage of what already works well today
- Proposals:
  - Trust building exercises
  - Physical meetings: one in the US, one in Europe
  - Share war stories
  - Organize a joint « security service challenge »
  - Re-instate cross-membership of one or two team members

Discussion

(and action list?)