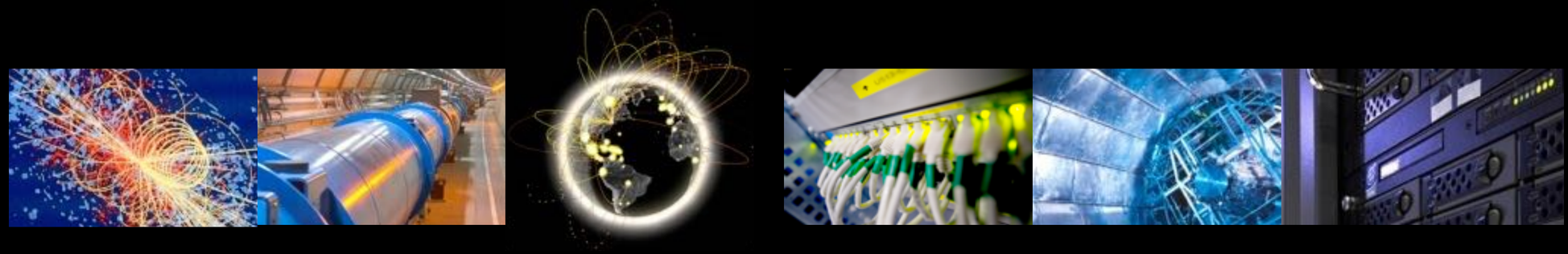
A word for "site" security teams



Romain Wartel

WLCG Grid Deployment Board, CERN, 9st May 2018

Things have changed

- When the grid started:
  - "Transparent arbitrary remote code execution across multiple administrative domains"
  - New software stack
  - New security model (authentication, authorization)
  - New operation model, including security (distributed teams)

- Result :
  - Most grid services put on a DMZ, or on a separate "scientific network"
  - Little trust and collaboration with central services

Things have changed

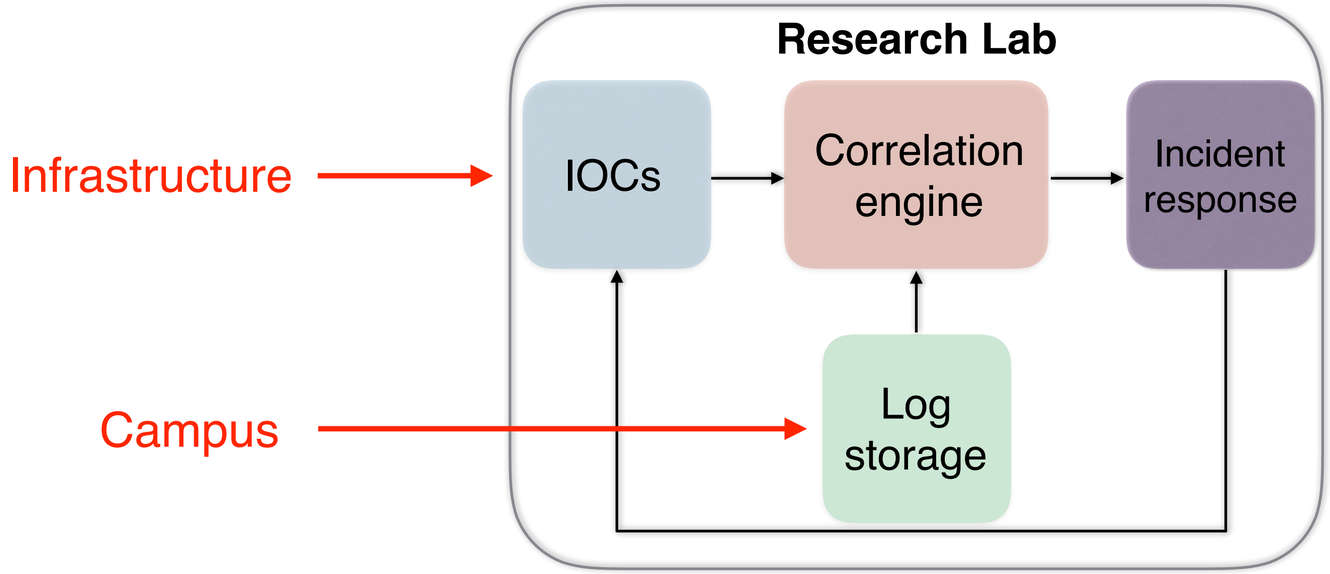
- 15 years later
  - Grid communities have very well organised security operations
  - Mature security operations, incident response expertise
  - Global network of trusted security contacts, actively sharing intelligence
  - Grid computing has helped make sites and the academic community more secure

- WLCG/EGI/OSG security teams have coordinated more than 100 intrusions in the last 10 years… None of them was caused by grid computing

- Grids and campus: same adversaries, similar risks
  - "Compromised identities are the most common intrusion vector for the security incidents that have affected WLCG. Attackers often initially capture credential on a weak service before propagating their attack further within our infrastructure by reusing the stolen credentials." – *WLCG risk assessment*

Complementarity

- Grids/clouds/infrastructures face traditional threats: criminal gangs, APTs, etc.
  - Malicious emails, drive-by, social engineering, etc.
  - Most of these infection vectors involve the main campus!
  - But grid security teams have no access to campus logs



- Sharing threat data, cooperating on security issues highly beneficial for all!
  - Cost saving, most efficient approach!

Collaborating, finally

- Share security operations?
  - Build trust, share details about intrusions, risks, incident response
  - Invite your grid security contact(s) to participate in campus security operations
  - Understand each other's top risks, strategy

- Integrate the "indicators of compromise" from grids/clouds/infrastructures
  - Directly in your SOC – Subscribe to the WLCG MISP instance
  - Participate in the WLCG SOC working group if you need help building your own SOC
  - Build your SOC with the help of grid experts!

- Aim at making grid computing "yet another IT service"
  - Network monitoring (IDS), syslog central storing
  - Start small, on the most exposed services (UI, WN, Web portal)