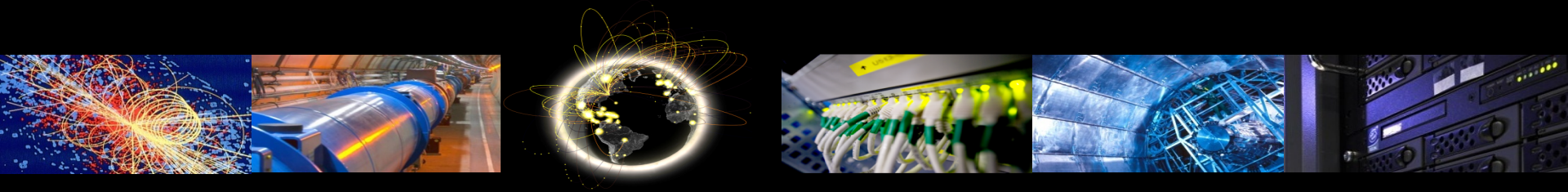
Risk landscape for the next 5 years

—

Security



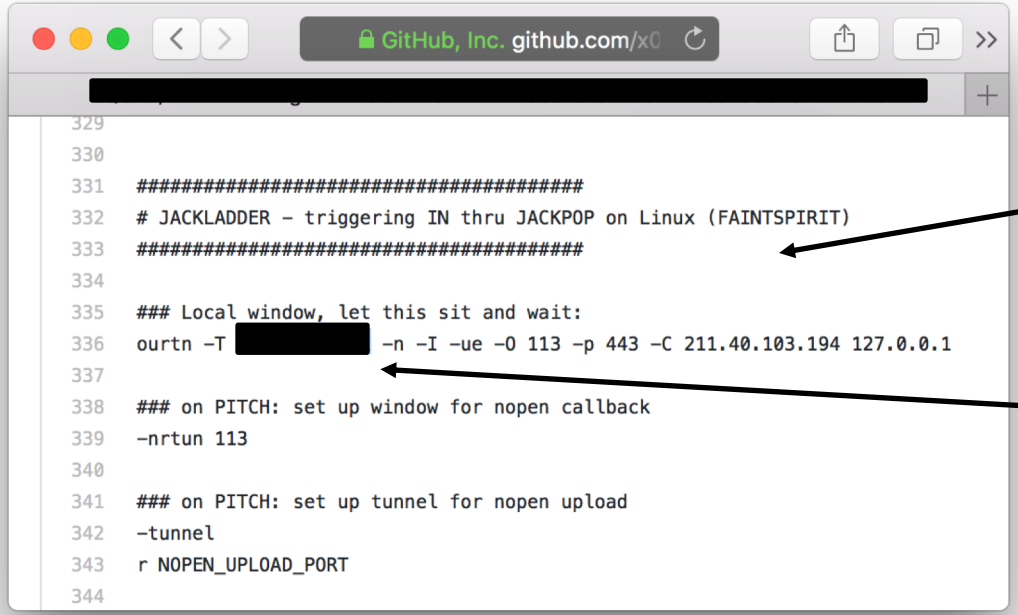
Romain Wartel, Joint WLCG & HSF Workshop 2018, Napoli, 26-29 March 2018

Coming soon: Infrastructure compromises

- More IaaS and PaaS attacks (not just underlying hosts)
  - Result: full infrastructure compromise
- Necessary to design systems assuming complete compromise
  - Aim at eradicating persistence
  - Continuously re-install systems, verify configuration, keep up-to-date with security patches
  - Design, implement and operate forensics-friendly systems
    - IaaS, containers, elastic resources, etc. TRACEABILITY is paramount
  - Implement fined grained access control, limit privileges (to delay lateral movement)
  - Limit amount of personal/sensitive data stored, use second factor authentication
- Evolving paradigm:
  - 2000's: Operate secure services (protection)
  - 2010's: Operate defendable services (detection)
  - 2020's: Operate resilient services (recovery)

Rise in government-sponsored attackers

- Governments need intelligence, information, … and computer resources
  - Goal: support national vendors, strategy, espionage, destruction, self-funding… or just test capabilities
  - "Science for peace" or open research does not mean HEP is not affected



leaked internal documentation of an *actively exploited backdoor?*

IP of a HEP organisation

IoT expected to cause major pain

- Huge rise in IoTs compromises and IoT-based attacks
  - IoT devices are perfect relays and proxies.
  - Expect significant increase in range of attack vectors
- Make sure your own IoT devices behave!
  - CCTV, printers, projectors, particule accelerators, Wifi access points, smart locks, coffee machines, thermometers, oscilloscopes, IP phones, etc.
  - Isolate from main network (best: fully disconnect), change default credentials, disable unnecessary services, keep up-to-date with vendor firmware.
  - Beware: most IoTs phone home, leaking local data. Sometimes impossible to disable!
  - Beware of Orphaned Network Traffic.
    - When an update domain of an IoT is no longer available at the end of the product lifetime
    - If an attacker buys the domain: “instant root”
    - Somfy, Honeywell alarms, phone manufacturers BLU, Infinix, IKU, etc. already affected

Criminal skills vs WLCG

- Average attack way beyond the skills of average WLCG site admin
  - Even for some basic, un-targeted attacks
  - Social engineering & vulnerabilities: endless infection vectors
  - Even advertisers are currently using malware-like domain generation algorithms (DGA)
  - Closely collaborating with your site(s) security team absolutely required
- Attackers:
  - Years of experiences
  - Evolved, modular malicious framework operated 24/7 over resilient infrastructures
  - No funding or staffing issue
  - Only need the victim to make one mistake or exploit a single vulnerability to succeed
- Get professional products, use frameworks and feed them indicators from friends

Proposed strategy for next 5 years

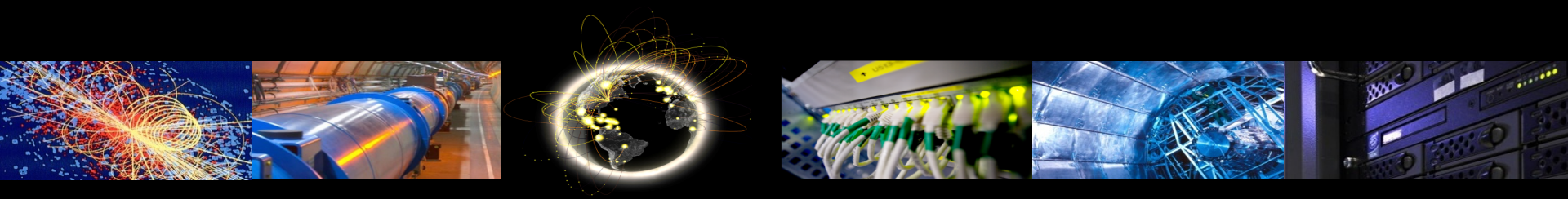
- Enable threat intelligence to be fully used by WLCG sites (See SOC WG)
  - Share quality threat intelligence among WLCG sites
  - Assist WLCG sites to implement appropriate SOC, IOCs and log correlation
    - Goal: receive, share and ACT on threat intelligence
- Convince site security teams to open up and collaborate
- Make security everyone's problem (and not a central team's full responsibility)
- Increase collaborations and build better trust relationships (globally and locally)
  - Other infrastructures, local government CERTs, private vendors, etc.
- Keep sites informed with malicious developments (GDB, vendors, training, etc.)
  - Improve sites security: email and desktop security, implement 2FA, « reinstall continuously », etc.

Operational Security

Incident Response & Traceability

V. Brillault

Joint WLCG & HSF Workshop, Naples: March 28th, 2018



WLCG
Worldwide LHC Computing Grid

CERN

Incident Response: Bigger and better?

- EOSC-Hub project:
  - Potentially joint EGI & EUDAT CSIRT
  - First step: unify procedures, communication
- AAI, eduGAIN, SIRTFI:
  - Incident simulation: lack of coordination
  - Need Incident Response policies, CSIRT?

Traceability: black boxes everywhere

- VOs will be running black boxes everywhere:
  - Full VMs: no visibility except network
  - Containers (incl. Singularity): limited visibility
    - No information about end-user!
    - Tracking execution/files not trivial
- Traceability is still possible
  - Sites: External behavior (e.g. network IDS)
  - VO: Users, user payloads

End-user traceability & suspension

- Split traceability model
  - Reduced experience, (very) few incidents
  - Organize challenges to maintain capability?
- Sites cannot block problematic users/payloads
  - Blocking unresponsive VO after 4h?
  - VOs should pull from emergency suspension

Container/VM images sources

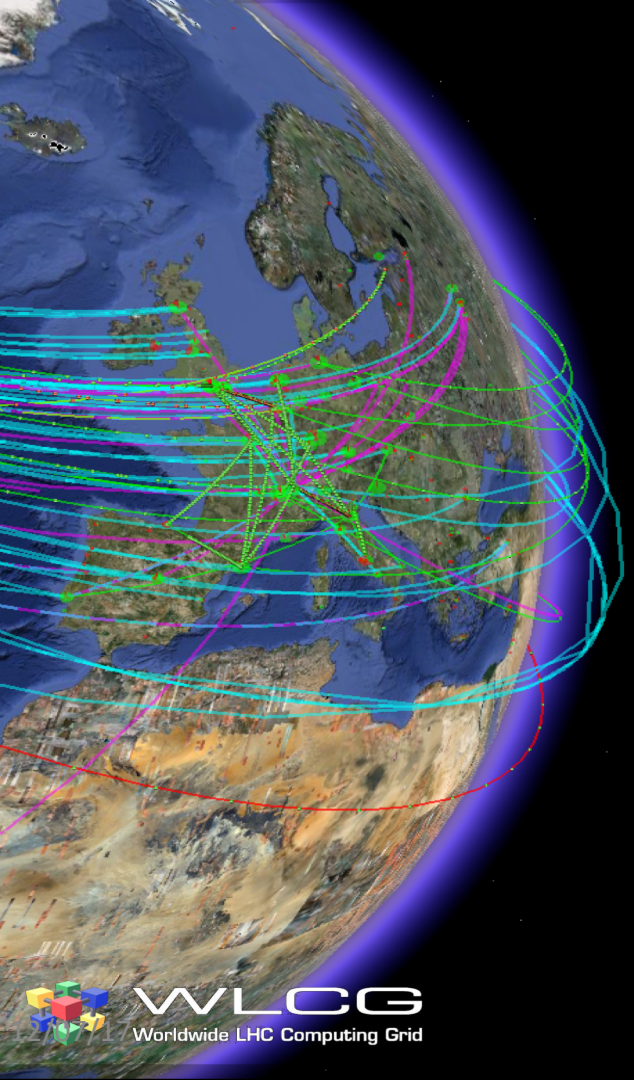
Two possible models for Container/VMs

	Maintained by VOs	Submitted by users
Adaptability/Features	• Stable & static • Limited built-in	• Full reproducibility • Full customisation
Traceability/debug	• Limited image space • Predictable behavior	• Short lived, multiple • Unpredictable bugs
Storage/cache	• Possible: few images	• Hard: many images • Caching layers?

Can we afford user-submitted containers?

Containers & Security

- RHEL7 *supports* unprivileged namespaces
  - As a technical preview only!
  - Long delays for security patches
- Singularity provides SUID *equivalents*
  - Plus access to *unsafe* root-only features
    - Block device mount, overlayfs…
- Unprivileged containers are not simple yet!



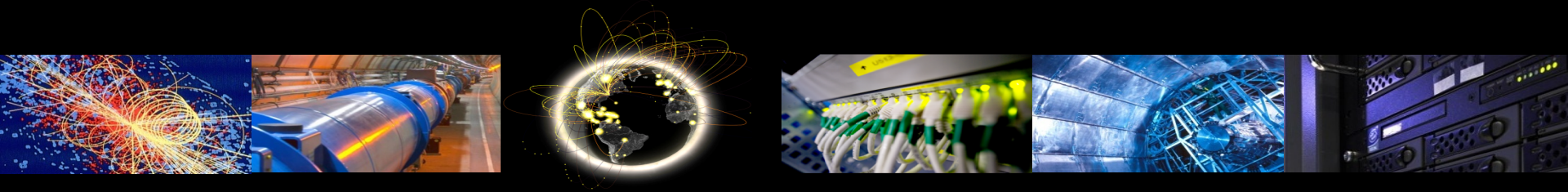
Short questions?

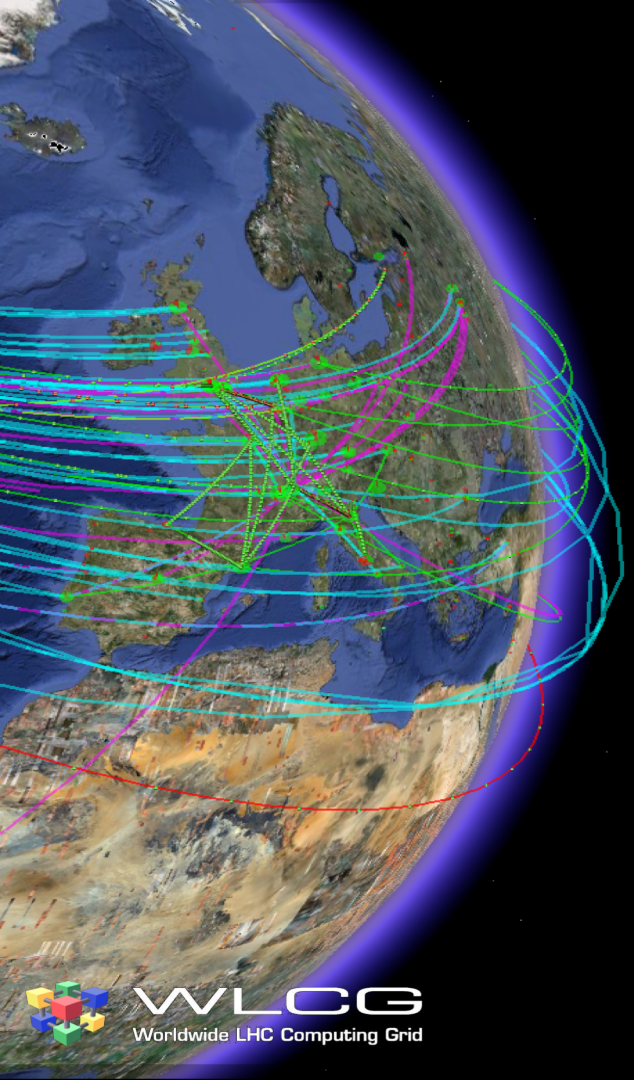
Discussions after next talk

Operational Security
Technology and Threat Intelligence

D. Crooks, R. Wartel, L. Valsan, V. Brillault, I. Collier

Joint WLCG & HSF Workshop, Naples: March 28th, 2018





Context

Basic premise

- Originally it was thought that grid sites would be a potentially major source of compromise
  - Had to convince campus security of trustworthiness
  - Acted to protect campuses/institutions

Reassessment

- In reality that hasn't turned out to be the case
- Grid security help resolve ~10 incidents per year which originated from non-middleware sources
  - *vs.* essentially none from middleware sources
- Last year, major threat to educational sites was ransomware
  - Phishing is the primary source of contamination
  - Increasingly difficult to distinguish from real email
  - SURF Cyber threat assessment 2017
- Grid sites only part of a much larger landscape

Revised goal

- Need closer collaboration/reevaluation of links between grid sites + campus security
  - Campus security: access to main network links
  - Grid security: experience, collaboration
    - and threat intelligence
- Especially in light of new operating conditions
  - Opportunistic resources
- Profound cultural change
  - Most campus security teams don't collaborate extensively

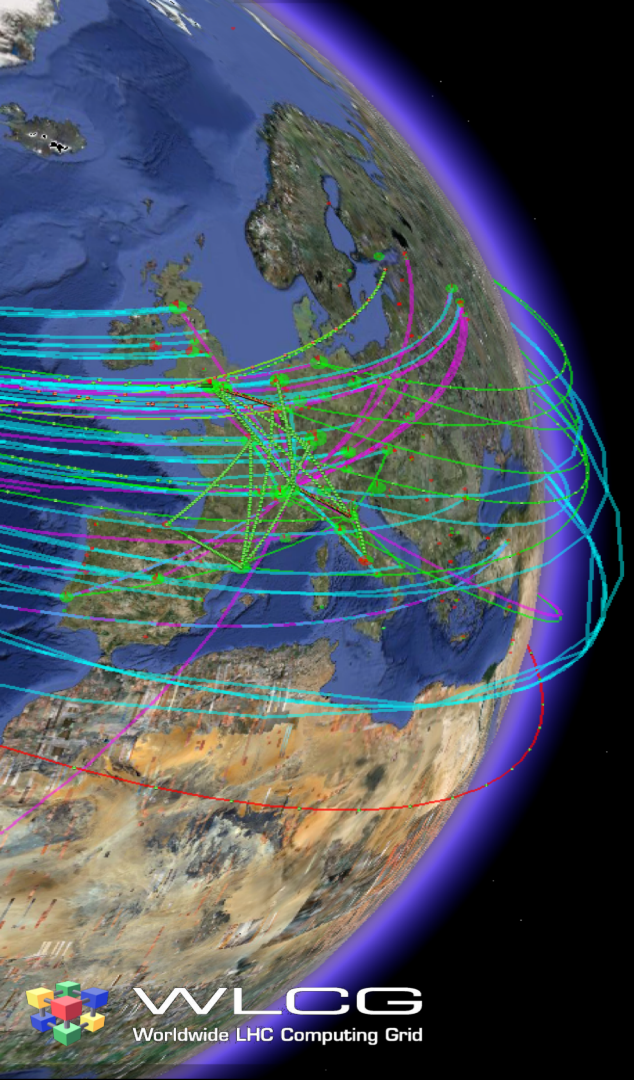
Threat Intelligence and Technology

- Opportunity to consider how we move forward in new computing context
  - Key questions

- What do we need?
- How do we get it?
- What do we have to offer?

What do we need?

Requirement	Effort needed now
Trust groups within our community	Less effort now but it took a long time to get here (15yrs)
Threat intelligence technology	Straightforward
Acting on threat intelligence	Very challenging



How do we get it?

Trust Groups within our community

- Trust groups that facilitate the sharing of threat intelligence within the community
- We have been working on these for a long time
- Experience in setting these up
  - Both inside and outside our community

Threat Intelligence Technology

- Malware Information Sharing Platform: MISP
  - www.misp-project.org
- In wide use in many communities
  - Academic, Industry, Government
- CERN security team has considerable experience
  - Upstream code fixes, adding features …
- WLCG instance in production, hosted at CERN
  - Access via eduGAIN+SIRTFI

MISP Deployment options

- Use WLCG instance as a base, with different modes of operation for sites
  - Remote access: site interacts solely through API, use WLCG instance as a web front end
  - Local installation (grid only): sites wishing to be more involved with WLCG events
  - Local installation (grid/region/institution): sites may have regional/institutional trust groups

Acting on threat intelligence

- Security Operations Centres (SOC) WG
- In existence since 2016
- Steady progress including recent workshop in December 2017
- Grow from basic reference components
  - Threat intelligence + network monitoring/IDS
  - MISP + Bro [www.bro.org]

SOC WG

- Growing membership
- December 2017 Workshop
  - Focus on deployment of MISP+Bro
  - 19 sites registered, ~12 in attendance
- All sites that tried installing MISP were successful
  - Now have 3 sites actively syncing with WLCG instance
- Similar number made progress with Bro
- Clear appetite for more in-depth sessions

Advert

- Next workshop at CERN: Registration open!
- https://indico.cern.ch/event/717615/
  - 27-29th of June 2018
  - 2.5 days
    - Initial steps
    - Network topology
    - Elasticsearch and associated tools
    - Advanced aggregation, correlation and enrichment of generated alerts

Two areas of work

- Technology stack
  - Technology needed to build a SOC
  - (starting from) Bro + MISP

- Social/cultural:
  - Social and cultural shift in sharing of intelligence
  - One goal of this group is to explore collaboration between grid and institute / campus security teams
  - Threat intelligence + collaboration

Two areas of work

- Technology stack
  - Making good progress
  - We are good at designing technical solutions
  - Definitely welcome new contributors

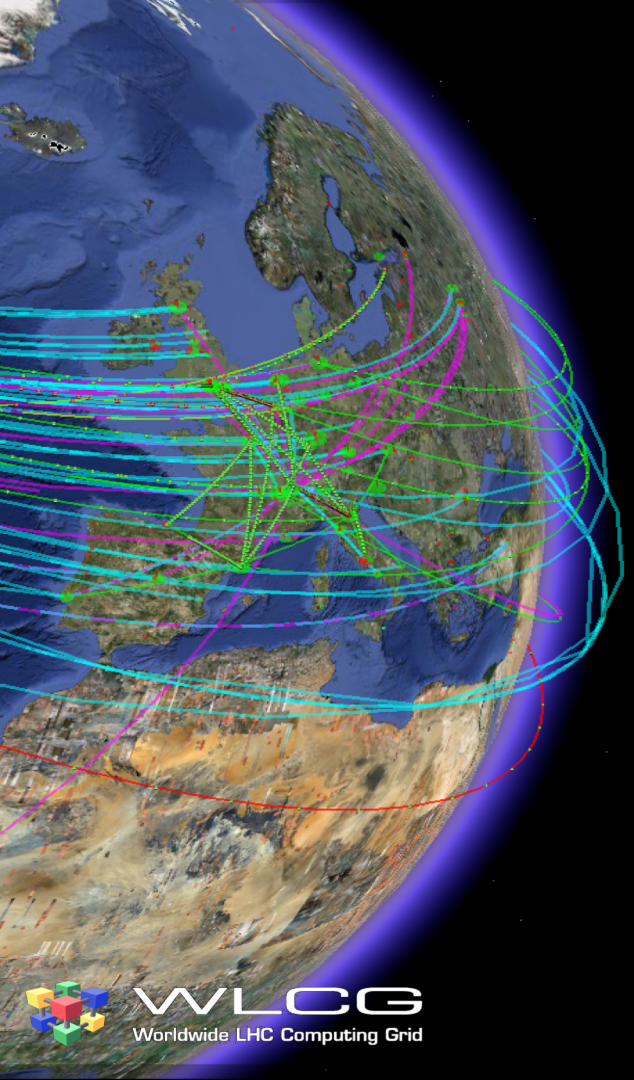
- Social/cultural:
  - This is much harder
  - Some individual/national efforts
  - How best to achieve this?

Next steps

- Continue technical progress in working group through workshops and discussions on mailing list
- Discuss specific requirements, including policy
  - Propose specific pre-GDB meeting
- Discuss how best to progress work with campus trust groups and cultural change
  - Here and at GDB

What can we offer?

- Experience
  - Years of building trust groups
- Collaboration
  - Structures like the WLCG that exist for this purpose
- Threat Intelligence
  - Build on existing security relationships



Conclusions and Recommendations

Conclusions

- Opportunity to rethink assumption that grid will be main source of compromise
- Much of the work to carry out the trust group part of this work is in place after years of effort
- Technical work is progressing, but would benefit from more participants
- Now need to extend that experience to campuses and institutions
  - This is challenging but not a new process

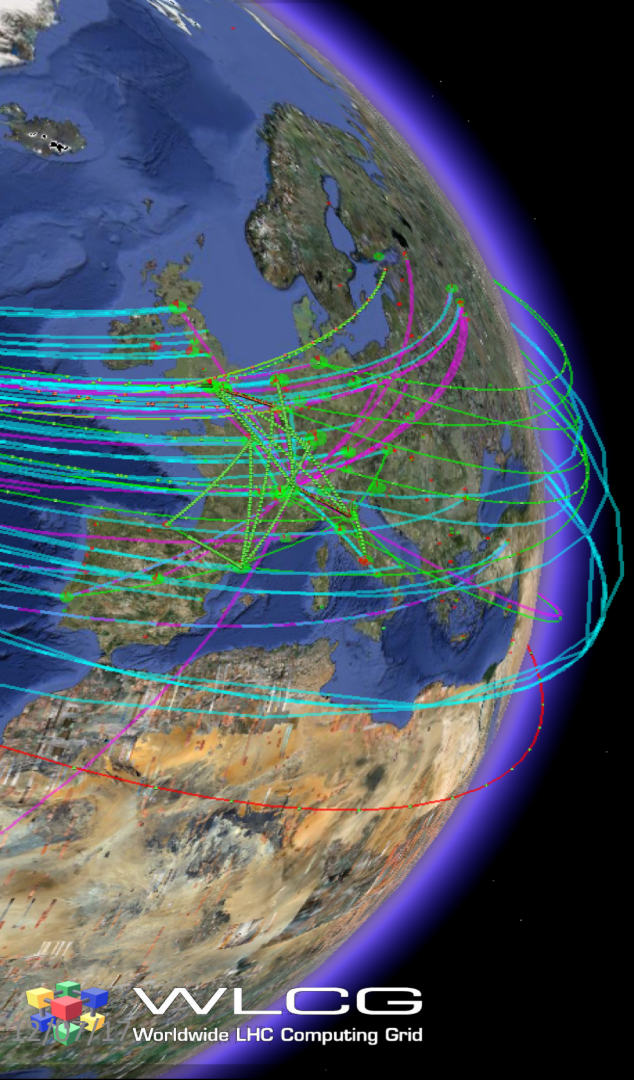
Recommendations

- Key recommendations at this stage

- We need collaborations and trust groups to share threat intelligence
- We need the technology to enable this
- We need the processes and culture in place to act on threat intelligence
  - This is challenging but essential

SOC WG Contacts

- Website
  - wlcg-soc-wg.web.cern.ch
- E-group
  - wlcg-soc-wg@cern.ch
- Documentation
  - wlcg-soc-wg-doc.web.cern.ch



Questions?