Site security challenges: some thoughts

Eygene Ryabinkin

National Research Centre “Kurchatov Institute”

EGI CSIRT meeting, CERN, January 30th 2018

Who do we target and what do we want?

Our audience:

- Site admins: they comprise the majority of our target audience.
- Site security contacts: as the coordinators of the incident response, but also as experts analysing incidents (helping site staff).
- VO people: central operations and regional ones.

What do we want people to be trained on:

- Site admins. The usual stuff: trace job/storage operations through the infrastructure, identify job processes, files on the storage. Network tracing also (Netflow/whatever).
- Security contacts. IR process, technical involvement to the lesser (?) extent.
- VO people: traceability from their side. Attacks on the core VO services: doable, viable?

НИЦ «Курчатовский институт»

The landscape

From last year's presentation:

- Resource landscape is somewhat changed: now we have clouds (even as official resources) and HPCs (mostly as unpledged, but, for example, Titan delivers to ATLAS millions of CPU-hours, around 7% of the whole MC production as of 2015).
- Other people/infrastructures are interested in doing trainings, events, etc: experience, software, best practices are good (cross-pollination, not just "we know it all").

For SSC: cloud/HPC resources are interesting, since they are really becoming common, so good to understand, if we can pinpoint them and either exploit (not in security sense) their specifics or just treat as the usual sites.

Technical side

- DIRAC: framework, used by LHCb, also by BioMed.
- Usual resources: CREAM CE, storage (DPM, dCache, xrootd, EOS, StoRM, BeSTMan).
- HPC, cloud: we seem to need them.
- Job submission: pilots everywhere (OK).
- Data access: storage systems, central catalogue, local disks. What happens on HPC/cloud resources?
- Usual WLCG workflow: for sure, LHCb.
- BioMed (and other VO)-specific worflows: do we want them? Can we realistically do that?

НИЦ «Курчатовский институт»

That’s all, folks!

Let’s brainstorm!

НИЦ
«Курчатовский
институт»