

Trust model between Experiments and Sites

SWRelease
CloudSquad HTCondor Users
Security LostHeartbeat DashBoard
Pilot R2D2 LifetimeModel
ObjectStore WallClock DAOD
AOD CloudProvider Analysis Tier-0
Dataset HTTP Yoda MonteCarlo ADCoS
BigData JEDI EventIndex C3PO DAST
APF AK47 DuplicatedEvents MadGraph
Rules PSS Rucio AMI DPM FAX PD2P WLCG
EGI FTS Deft
xrootd HPC dCache ATLASComputing
C-RSG HIST RSS EventService arc
RAW Memory Panda Reprocessing Trust
Hadoop Federation Efficiency Batch
Analytics Sites EVNT
CVMFS arcCE
HammerCloud DerivationFramework
StorageConsistency
Kibana Condor



Alessandro Di Girolamo

CERN-IT

Trust Model: Experiments and Sites

- Bilateral trust
 - Sites trust Experiments
 - Experiments trust Sites
 - But not only: also experiments and sites trust their users
- Working together
 - Trust works best between individuals
 - Unrealistic to have sufficient expertise from all the involved partners:
 - fundamental to build the Trust together



A real example: bitcoin mining (Dec 2013)

- **9:43am:** A site admin, after having noticed “strange” processes on one of its WNs, contacted the ATLAS security contacts
- **11:30:** User is banned from ATLAS
- **12:30:** User contacted and incident fully understood. ATLAS experts have in the meanwhile identified all the affected jobs (which started that same morning at 2am)
- **15:43:** Official announcement with the description of the complete (already closed) incident to WLCG-security contacts

excerpt

Site - Experiment Security contacts - WLCG security team

Security is based on collaboration, it relies on the trust between the players

Do we have an issue?

don't think so!

but...

- Reputation is always at stake
 - Not only for “real” security incidents
 - very difficult to control the flow of the “rumors”



?!?

Hacker all'assalto delle banche greche. "Riscatto in bitcoin o salta tutto"

L'Armada Collective - già autore di iniziative [contro il Cern \(che ha pagato\)](#), in Svizzera e Thailandia - ha disattivato per mezz'ora il sistema di uno dei quattro grandi istituti, domandando 17mila euro in criptomoneta per non far saltare tutti i circuiti. Ma l'intervento delle autorità creditizie ha consentito (per ora) di sventare l'attacco informatico dei pirati telematici