EGI-CSIRT/LHCB F2F Apr. 2018

EGI-CSIRT

EOSC-Hub

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142

SSC Dirac

Subsection 1

SSC DIRAC Status Meeting 26. April 2018

DIRAC SSC Checklists

Operations:

- Identities (Testing, SSC), x509 certificates/keys, passwords availvable to Redteam ?
- Dirac UI, ready to use, tested with SSC identities ? (Chris/Sven)
- SSC Monitor up/running ? (Aram)
- Jobcontrol in SSC-Mon (start/stop) via dirac and ”glite-job-submit” tested? (Sven/Aram)
- Bots connect back to cnc via tor
- Ban Monitor functional tests (Central, site (Nikhef), VO)? (Sven)
- Malware (Miner/dosser) available ? (Eygene)
- Malware (miner/dosser) tested? run jobs at Nikhef/CERN (Sven/Chris)?

DIRAC SSC Checklists

Operations:

- Timelines for incomplete Operation Items?

DIRAC SSC Checklists

Scope

- Participating Infras (EGI, WLCG, more?)
- Participating Sites (List) ?
- finalize Scope

DIRAC SSC Checklists

Incident Response

- Incident Response Procedure DIRAC
- Incident Response Procedure IRTF
- Sufficient hooks for collaboration? Potentially conflicting steps?
- Tested communication endpoints in both teams?
- IR at Sites: Documentation for site admins? (how to get to the real payload, suspend id?)
- IR at VO: Documentation to secure malicious payload, find attacker ID, suspend attacker ID, control running attacker jobs.

DIRAC SSC Checklists

Report:

- Define Site, VO IR-Performance indicators.
- Report: What the forensics results should have been (Eygene, Aram)
- Report: What the containments results should have been (Vincent, Chris)
- Report Generator (Draft Sven, tex-foo needed)