EGI-CSIRT Operational Security

Sven Gabriel

Operational Security Update

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

Critical Vulnerabilities

- Various, no new CRITICAL Vulns

Incidents

TLP:AMBER EGI-20171213-001

- Reported by Site Admin
- Crypto Currency mining activity
- Attack vector under investigation

EGI-CSIRT / EUDAT F2F Meeting Nov 2017, Helsinki

Agenda Day-1

Agenda:

- Thursday:
  - Summary last F2F (brief)
  - Security in EUDAT
  - Security in EGI (Intro + Updates from the activity groups)
  - Lunch
  - EOSC-Hub Proposal
  - EOSC-Hub Proposal / Outreach (Web, DI4R, ISGC, etc)

Summary Day-1

Joint Presentation at DI4R:

- EUDAT Security Officer observing member in IRTF
- Evolution and Status EGI-CSIRT and EUDAT Security
- Next steps in collaboration, Integration

EUDAT EGI-CSIRT Coordination Integration I

- Policy
  - Full cross-review, alignment, and create road-map.
  - AUP alignment & GDPR are early priorities.
- Procedures
  - Alignment of the Incident Response Procedures.
  - Ensure maintained contact details to all sites are available.

EUDAT EGI-CSIRT Coordination Integration II

- Incident Response
  - EUDAT Security observing member in EGI-CSIRTs IRTF
- Incident Prevention
  - Monitoring EGI and EUDAT teams to review options for collaboration.
  - Vulnerability: SVG will investigate possible collaborations.

EUDAT EGI-CSIRT Coordination Integration III

Next joint F2F scheduled for 29 – 31 Jan. 2018

Agenda Day-2

Agenda:

- Friday:
  - FedCloud Security Status
  - FedCloud Security, Certification, Trainings
  - Positive Certification of FedCloud Services

Summary Day-2

- FedCloud Usage/Status
  - FedCloud Usage: Stability/Usage increased
  - predicted future usage through Services Galaxy, Juniper, Kubernetes etc
- Training/Certification
  - 2 Base (Foundation) Trainings to be delivered in 2018
  - First Training scheduled for ISGC (March 2108)
- Service Certification
  - In FedCloud Users use heavy services processing user credentials etc, creating a compute clusters, with unclear relation to EGI/EGI-CSIRT.
  - Users need to be able to selec ”certified services”
  - No heavy certification with external reviewers/auditors needed, this will be done by EGI-CSIRT.