EGI-CSIRT Operational Security

Sven Gabriel

CSIRT F2F, summary, planning

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

Security Trainings

EGI Service Catalogue:Security Trainings

EGI CSIRT Trainings:

Defensive: Protect your (grid-)site while under attack. (Leif Nixon)

Offensive: Scan for Vulnerabilities, attack! (Leif Nixon, Daniel Kouril)

Security tools/monitoring: install configure security monitoring in a training env.

Forensics: This VM got compromised, find out what happened. (Heiko Reese)

Role Play Training: Address new technologies/services in a *What if* scenario, can be combined with *Hands-On*

EGI Service Catalogue:Security Trainings

- Some of the Trainers left the project, may still be available.
- Currently looking into *Train the trainers*.
- Need constant development to address new technologies.
- Currently developing a training targeting Orchestration Services.
- . . . **in collaboration with ASGC security experts**.

SSCs

FedCloud SSC, status

- New group of contributors, migrated Nikhef Subversion Repo to GIT ACL easier to maintain.
- Documentation on SSC-Monitor in progress
- Implementation of VM management (start/stop) in SSC Monitor challenging.
- Depends on Command Line tools to start/stop VMs
- With expert help we can now reach 5 sites, sites are very heterogeneous!.
- Agreed on: Do a SSC with the sites we can reach.

SSC Future Developments

- Key developers left the project, new people needed.
- Eygene is interested to participate in the SSCs
- Targets: VO WMS's (DIRAC, Alien, etc)
- Project started.

FedCloud Security

FedCloud Sec

- Remote participation: Vincenzo, Giacinto
- Vincenzo presented on IM (thanks!)
- Basic discussions on Orchestration / Contextualisation
- Identified security issues (maintaining/endorsing templates) Endorsement policy etc

Incident Debriefings I

- Communication channels not sufficient
- FedCloud user communities not yet sufficiently represented in the relevant security activities.
- Indigo/FedCloud should have reps in SVG RAT.
- New services should follow best practices before being used.
- Software validation/ egi quality control, re-use UMDs tools/processes

Incident Debriefings II

- Short Term: Security Audit of IM, need support from EGI Management.
- Fix most urgent security issues.
- Long Term: Policies, Procedures, Maintenance, Quality assurance/control to cover Cloud services (Ex. Orchestration).