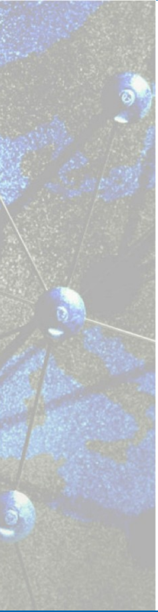

EGI-CSIRT – Operational Security

Activity Update

EGI-CSIRT

sveng@nikhef.nl, Nikhef, EGI-CSIRT

EGI-CSIRT OMB 18. Dec. 2014

Activity Update

- Security Operations: Incidents / Alerts, Advisories
- Cloud Security
  - Evaluation of the questionnaires
  - Closer collaboration FedCloud EGI-CSIRT / Fedcloud F2F Jan 15
- Collaboration EGI-CSIRT/WLCG: Pakiti and MW Readiness WG
- Central Suspension

EGI-CSIRT OMB 18. Dec. 2014

Security Operations: Incidents / Alerts, Advisories

- Critical Vulnerability, kernel upgrade needed before Christmas Break https://wiki.egi.eu/wiki/EGI_CSIRT:Alerts/Linux-2014-12-17
- Incident 7782: ddos attack affected EGI services
- Incident 7765: security incident at site ARNES (Very good response from local Security Team)

EGI-CSIRT OMB 18. Dec. 2014

Cloud Security, Evaluation of the questionnaires

- Summary: EGI Conference on Challenges and Solutions for Big Data Processing on Cloud, 24-26 September 2014
- Detailed Feedback in preparation, format wiki page.

Cloud Security, EGI-CSIRT/FedCloud collaboration

- Cloud Incident triggered various weak points, EGI-CSIRT needs a Cloud Tech expert with security background (Boris Patrak, CESNET), needs to be formalized.
- Boris presented at the EGI-CSIRT F2F 15 - 17 Dec 2014
- EGI-CSIRT / FedCloud need to coordinate on the Agenda for the FedCloud F2f in Jan 2015
- Goal: identify/solve operational problems in Incident Response (ex: traceability, central control over running vms)

EGI-CSIRT OMB 18. Dec. 2014

Collaboration EGI-CSIRT/WLCG: Pakiti and MW Readiness WG

- Headed by Daniel Kouřil
- WLCG wants: Controlled deployment of WLCG middleware across sites. Monitoring of packages installed on sites with Pakiti
- Problem: Access to the aggregated software packages information (sensitive data)
- EGI has strict rules on accessing pakiti data, WLCG-OPS can not easily be included here.
- Solution: 2 collector instances (EGI-CSIRT, WLCG-OPS), Sites decide where to send the data.
- Detailed presentation at a later OMB by Daniel Kouřil

EGI-CSIRT OMB 18. Dec. 2014

Central Suspension, Status ?

- Phase 1 (from OMB 18. Sept 2014)
  - NGI Argus Services are deployed (coordinated by EGI Operations, action on NGIs, ggus tickets opened)
  - Information of the NGI Argus services is in the appropriate format in goc db (action on goc-db/NGIs, coordinated by EGI Operations)
  - Monitoring that NGI-Argus services have updated banning information, monitoring results available to EGI-CSIRT for example via security dashboard (coordinated by EGI Operations, action on Nagios Monitoring group)
  - Remark: probe is available from V. Brillaut
- Test if ban information propagates to the sites services: CE/SE/WMS (action on EGI-CSIRT)
- icinga2 server installed, NGI NL hosts configured, probe