EGI CSIRT 2012 Plan

Overview

- Daily operation
- Security Service Challenges
- Security Monitoring
- Security Training and Dissemination
- Other CSIRT activities

Daily Operation

- Security Officers On Duty on Weekly Rotas
  - Weekly operation meeting
    - Monday 10:30 (CET) on EVO
    - Weekly report in EGI CSIRT private wiki
  - 10 NGIs security officers and their backup
    - Czech NGI, Dutch NGI, German NGI, Greece NGI, Ireland NGI, Poland NGI, Portugal NGI, Spain NGI, Sweden NGI and UK NGI
- Response to any reported security incident
- Assisting sites to solve any critical vulnerabilities (flagged by monitoring tools)

Security Service Challenges (SSC)

- SSC5 EGI run was completed in June 2011, in total 40 EGI sites participated
- SSC will continue in 2012
  - Detail plan on following slides

Like a fire drill!

SSC5 Framework Improvement

- SSC5 Framework will be used by NGIs
  - To integrate more job-submission methods
    - ATLAS panda had been fully integrated
    - Globus, gLite job submission and VO-Job-Submissions-Frameworks (as needed) will be integrated by Q2 of 2012
  - To address the scaling problem of Access Monitor Module by Q1 of 2012.
    - This module tests if a certain x509-proxy can be used to access services at a site (ban-monitor)
  - To address issues found in the reporting module during the SSC5 EGI run

SSC5 Regional Run in NGIs

- To pilot the regional run in at least one NGI in Q1 of 2012
- EGI CSIRT will assist NGI security officers for their regional runs after the initial pilot
    - To run SSC5 in your NGI, please ask your NGI security officer to contact EGI CSIRT

SSC6 Plan

- SSC6 will be similar to SSC5 EGI run
  - Use another VO-Job-Submission-Framework
  - It will simulate a security incident to test sites, VO and CSIRT incident response capabilities and their collaboration
  - Preparation will complete by Q2 of 2012
  - SSC6 is expected to launch in Q3 of 2012
  - Evaluation of SSC6 results will be completed and made available to participants in Q4 of 2012.

Security Monitoring

- Security Dashboard
  - https://operations-portal.egi.eu/csiDashboard
- Further development & improvement
  - Expect to be in full production in Q1 of 2012
  - Expect to implement an initial security alert handling workflow by Q2 of 2012
  - Expect to produce regular security metric reports (monthly or quarterly) by Q3 of 2012

Security Monitoring

- Pakiti
  - A new version of Pakiti (Version 3) is expected to be released in Q2 of 2012
  - http://pakiti.sourceforge.net/ for more information
- Site wide security monitoring
  - To monitor site patching status via job wrappers or other mechanism;
  - To identity feasible solution, produce implementation plan and proposal by Q2 of 2012

Security Monitoring

- Nagios security monitoring
  - Migrate CSIRT Nagios box to egi.eu domain
    - No service interruption is expected.
    - To be completed by Q1 of 2012
  - Continue improving the backend Nagios-based security probes.
    - CRL and known vulnerable file permissions checking via Gridftp
    - Expect to be implemented by Q4 of 2012;
  - Exploit the possibility of adding more security probe for other services

Security Training & Dissemination

- Security trainings at EGI TF 2012 is planned
  - If possible, will join effort again with EMI security team
- To maintain and continue improving EGI CSIRT wikis, assisting best practice document development

Other CSIRT Activities

- Two EGI CSIRT face to face meetings
  - 1st meeting at Bologna(CNAF), Italy on 23rd -24th April 2012
  - 2nd meeting at 2012 EGI TF
- Monthly team meeting (online)
  - https://www.egi.eu/indico/categoryDisplay.py?categId=23
- Security operational procedure development
  - Add security check to site certification procedure PROC09 (https://wiki.egi.eu/wiki/PROC09), to be done in Q3 2012
  - Define new procedures (such as Operational procedure for Certificate compromise) and updating existing ones if needed
- keep track of development in areas of identity federation, IPv6 security and cloud/virtualization security