

# EGI CSIRT Meeting

Mingchao Ma

- House keeping stuff
- EGI global task review (MS115)
- EGI risk assessment
- EGI federated cloud
- EUGridPMA SHA1 risk assessment
- EGI CSIRT 2012 roadmap review
- Preparation for EGI TF 2012

- Fire alarm?
- Lunch and coffee break
  - Coffee break at 10:30 and 15:00
  - Lunch at 12:30 for an hour
  - Any other house keeping stuff?
- Minutes taker

- Milestone 115
  - A self-assessment of the EGI Global Tasks from a managerial perspective
    - <https://documents.egi.eu/document/961>
    - Based on NGI feedback/score
  - A score ranging from 1 to 5
    - 1 = unacceptable; 2 = below expectations 3 = acceptable; 4 = exceeded expectations; 5 = an excellent service
  - Coordination of Operations Security scores 4
    - EGI CSIRT and EGI SVG
  - Security monitoring scores 3.8

- EGI Delivery 4.4 and risk assessment
  - A slightly detailed than WLCG risk assessment
  - To be ready for Y2 review in June 2012
  - First version need to be ready by end of April
    - Otherwise reviewer can reject the document
    - But amendment can be made if necessary
  - Individual risk assessment done
  - Meeting on 20<sup>th</sup> April after the assessment
    - ?

- EGI federated cloud task force
  - <https://wiki.egi.eu/wiki/Fedcloud-tf:FederatedCloudsTaskForce>
  - Interesting discussion at EGI CF 2012
    - <https://www.egi.eu/indico/sessionDisplay.py?sessionId=37&confId=679#20120329>
- What should EGI CSIRT do?
  - Any experience?
  - Best practices?
  - ?

- Already start, aiming to complete before EUGridPMA/IGTF all hands meeting in May
- EGI CSIRT
  - Contribute to the risk assessment
  - Understanding the implication of the result
    - What (e.g. procedure?) the EGI should do if SHA1 was suddenly broken?

- Q1 revisit
  - 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)
  - SSC5 regional run in NGIs, to pilot at least one NGI run in Q1 of 2012, and assist NGI security officers for their regional runs after the initial pilot
  - Security Dashboard further development & improvement based on gathered feedback, expect to be released in Q1 of 2012
  - Migrate domain name of CSIRT Nagios box from current `srv-102.afroditi.hellasgrid.gr` into `*.egi.eu` domain (e.g. `secmon.egi.eu`).



- Q2
  - CSIRT face to face meeting
  - RTIR hands-on training
    - Improving issuing handling with RTIR and any further improvement
  - To extend SSC5-framework and 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
  - The SSC6 preparation
  - To define and optimize security alerts (as shown in security dashboard) handling workflow, explore the possibility of integrating non-critical security operation into normal day to day operation, expect to implement an initial workflow by Q2 of 2012
  - Pakiti (Version 3) is expected to be released in Q2 of 2012
  - site-wide security monitoring (patch monitoring); To identity feasible solution, produce implementation plan and proposal by Q2 of 2012

- Q3
  - Security service challenge 6
  - Site certificate procedure update
  - Security training at EGI TF 2012
  - Operation procedure for compromised certificate/CA
  - To define some basic security metrics, which are calculated through security dashboard; expecting to produce regular security metric reports (monthly or quarterly) by Q3 of 2012

- Q4
  - Evaluation SSC6
  - nagios: CRL checking on services that have gridftp (CEs/SEs) and checking for known vulnerable file permissions via gridftp
- Ongoing activities
  - Daily operation and Incident handling
  - SSC5 NGI runs
  - Issuing handling improvement
  - Meetings
  - Identify federation, IPV6 and Cloud security

- Face to face meeting
  - 3 hours, two sessions
  - Possibility for a breakup meeting
    - More than 3 hours
      - But how long?
    - To find a suitable time
      - All/most members are available
    - And a meeting room
  - Any view on the breakup meeting?
- Security training
  - Two sessions and joint effort with EMI?

- Term of Reference
  - <https://documents.egi.eu/document/385>
  - No further comment received
- EGI CSIRT membership management
  - EGI CSIRT member
    - [Egi-csirt-team@mailman.egi.eu](mailto:Egi-csirt-team@mailman.egi.eu)
  - IRTF member
    - [csirt@mailman.egi.eu](mailto:csirt@mailman.egi.eu)
  - On duty rota: a special SSO group
  - NGI security officers
    - [Ngi-security-contacts@mailman.egi.eu](mailto:Ngi-security-contacts@mailman.egi.eu)
  - Site security contacts
    - [Site-security-contacts@mailman.egi.eu](mailto:Site-security-contacts@mailman.egi.eu)
  - External partner/grid representative
    - [Site-security-contacts@mailman.egi.eu?](mailto:Site-security-contacts@mailman.egi.eu)