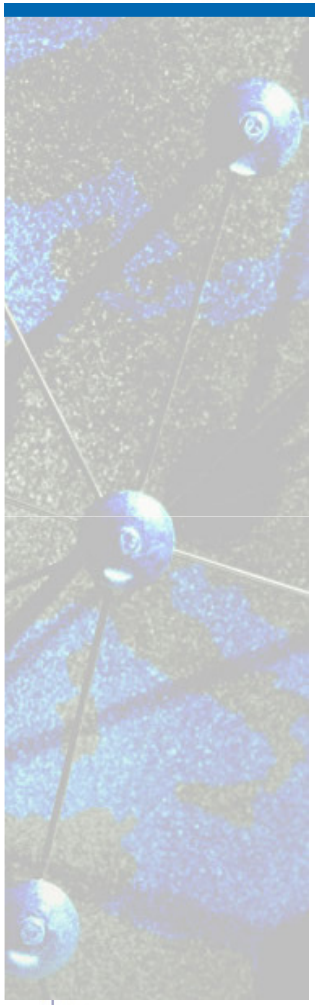


EGI – Computer Security Incident Response Team (CSIRT)

Dr. Mingchao Ma
STFC – Rutherford Appleton Laboratory
UK

Overview

- About the Project
- About EGI CSIRT
- Challenges and Issues
- Further Plans

About the Project

- Consortium Agreement agreed
- Grant Agreement signed
- New branding of EGI project
  - Logos, templates … …
- EGI User Forum, April 2011
- Milestone 405
  - Completed PMB review
  - https://documents.egi.eu/document/47
    - Security Incident Handling Procedure
    - Vulnerability Issue Handling Procedure
- The EGI CSIRT logo

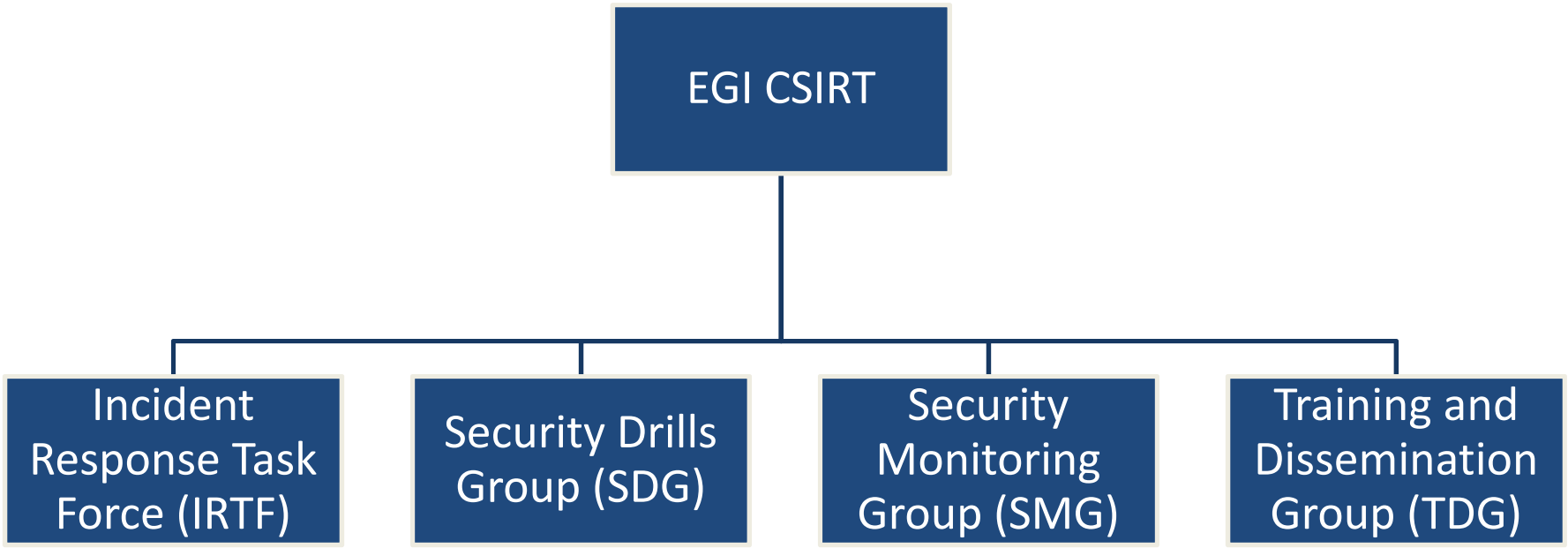
EGI CSIRT

- Coordinating the operational security activities in the infrastructure, in particular the response to security incidents
- EGI CSIRT combines efforts and resources from NGIs, each NGI must appoint a NGI security officer and provide NGI CSIRT function

CSIRT Members

- NGIs
  - Czech Republic NGI
  - Dutch NGI
  - France NGI
  - Greece NGI
  - German NGI
  - Ireland NGI
  - Italy NGI
  - NDGF NGI
  - Polish NGI
  - Portugal NGI
  - Spanish NGI
  - Switzerland NGI
  - UK NGI
- EIRO
  - CERN
- Asian Pacific Region
  - ASGC

Internal Structure



https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page

EGI CSIRT Activities

- Incident Response Task Force (IRTF)
  - EGI CSIRT duty contact rota
  - Security incident reponse
  - Security incident management
    - Communication channels
    - Incident response tools development, evaluation and adaptation
    - Incident handling procedures update/maintenance
  - Vulnerability assessment

- Security Monitoring Group (SMG)
  - Pakiti development and maintenance
    - https://pakiti.cern.ch/
  - Nagios-based security monitoring framework development
    - https://srv-102.afroditi.hellasgrid.gr/nagios/
  - Explore other security monitoring tools

EGI CSIRT Activities

- Security Drills Group (SDG)
  - Design, set-up and run SSC (security service challenges)
  - Evaluate and disseminate the result of security drills
  - Provide a framework so that NGIs can run a particular security drill at some or all of their sites
- Training and Dissemination Group (TDG)
  - Maintain EGI CSIRT public and internal wiki
  - Plan and organize training events
  - Collect and archive training materials used in past events
  - Support NGIs setting up local training events?
  - Develop training material?

Internal Communications

- Internal Communications
  - Regular online meetings
    - Weekly IRTF meeting
    - Monthly team meeting
  - Team mailing list
  - Internal Wiki
  - RT
  - Face to face meetings

External Communications

- Public Wiki
  - https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page
- Site security contacts mailing list
  - Production site CSIRTs
- NGI security contacts mailing list
  - NGI security officers/deputies
- Security incident report
  - csirt@egi.eu
- Collaboration with other teams/groups, peer Grids, NREN's CSIRTs etc.

Security Groups in EGI

Security Groups at EGITF

- EGI CSIRT face to face meeting
- EGI SVG session on Wednesday
- EGI SPG session on Thursday
- Open Security Forum on Thursday
  - SCG, SPG, SVG, EUGridPMA and EGI CSIRT
- Security training session on Friday

Current Issues/Challenges

- Multiple middleware stacks
- Large discrepancy of NGI commitments
  - From ~3PMs to ~40PMs over 4 years
- Internal procedures
  - Vulnerability/risk assessment
  - Ticket system (e.g. RTIR) for incident response?
- New incident handling procedure
  - Change of information flow, what is the implication?

Current Issues/Challenges

- Security monitoring and problem escalation?
- How better to use EGI RT and GGUS?
- More mailing list?
  - egi-csirt-discuss?
- Use of encryption in communication
- Patching criteria and patch management
  - Leverage power of VO and COD
  - Name and Shame

Further Plans

- Maintain normal operation
- Finalize and agree group activities plans now or in coming weeks
- Internal and public wikis
- Complete EGI CSIRT Term of Reference
- Improve internal procedures
- Address listed issues

AOB

- Next face to face meeting
  - Volunteer host?
- Tonight dinner