# Introduction of the EGI-CSIRT

*Sven Gabriel (Nikhef)*
*EGEE Operational Security Coordination Team*
*http://cern.ch/osct/*

www.eu-egee.org

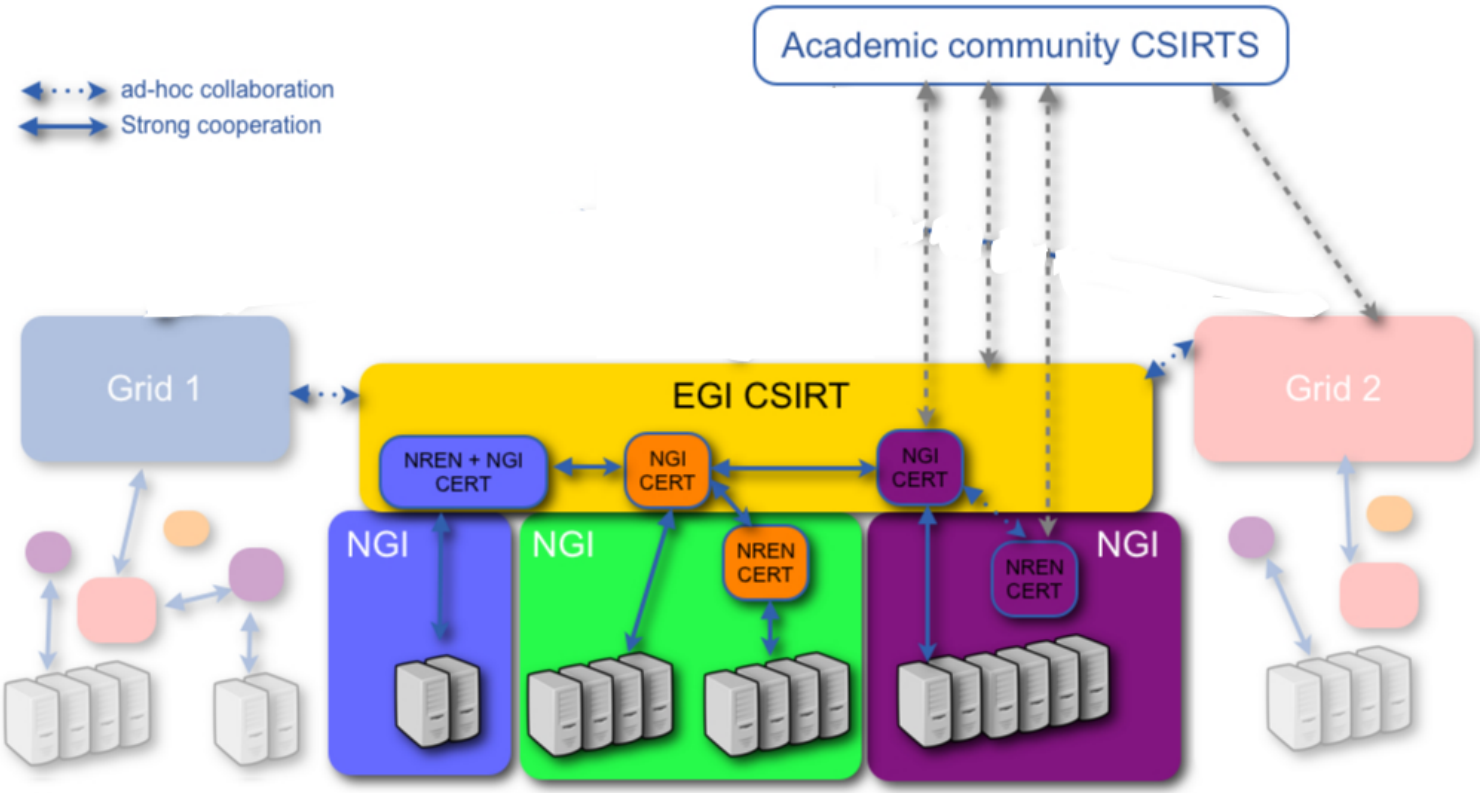
# Outline

- EGI-CSIRT: Mission, Tasks
- NGI Requirements
- EGI-CSIRT Groups
- EGI-CSIRT Groups kick off presentations, Applications welcome!

# EGI-CSIRT Mission

The main objective of the EGI CSIRT is to provide the EGI infrastructure with incident response capabilities across the participating NGIs.

# EGI CSIRT


Academic community CSIRTS
ad-hoc collaboration
Strong cooperation
Grid 1
EGI CSIRT
Grid 2
NREN + NGI CERT
NGI CERT
NGI CERT
NGI
NGI
NREN CERT
NREN CERT
NGI

# EGI CSIRT

- EGI-CSIRT aims at coordinating the operational security activities in the infrastructure.
- Implement procedures, technical means and appropriate communication channels to other CSIRTs.
- Provides a framework for the NGIs to help them to coordinate the operational grid security within the NGIs
- Overall security depends on the NGI-CSIRTs.

# NGI-Security-Officer Requirements

NGI-Security-Officer provides NGI-CSIRT function

- Coordinate the grid security activities in the NGI.
- Act as the contact point for security issues in the NGI for the rest of the infrastructure. (Back up ?)
- Maintain proper communication infrastructure to the sites in your country.

# NGI-Security-Officer

- Establish an environment within the NGI so that proper Security-Incident-Handling is ensured.
- Make sure the sites in your country know you and your function.
- Ensure proper investigations are done at the sites.
- Make sure sites have a Incident-Response-Procedure, (http://osct.cern.ch).
- Enforce local and project wide policies.
- Provide regional (security) monitoring.
- Contribute/Participate in EGI-CSIRT groups.

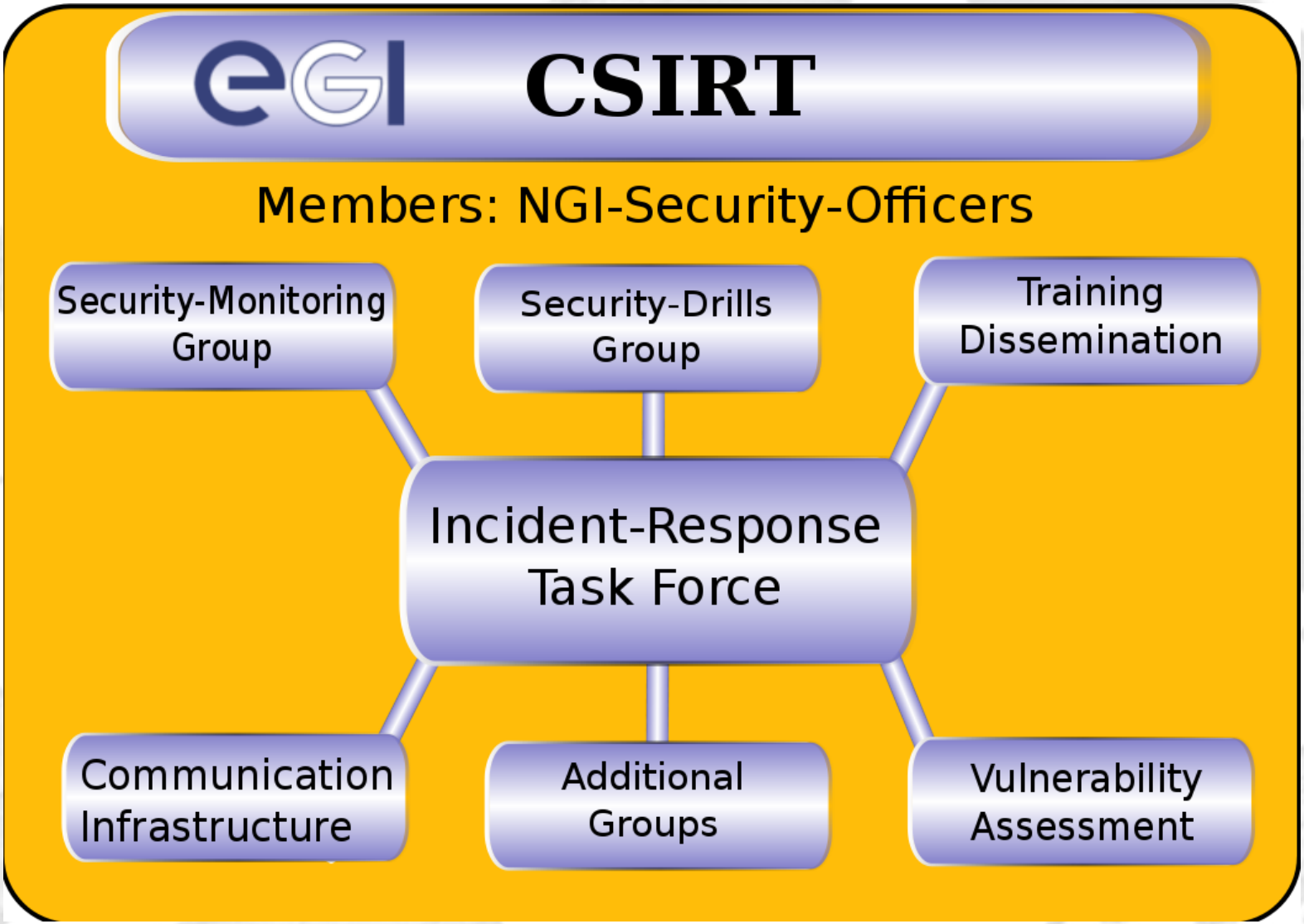
# NGI-Security-Officer

- Have a escalation procedure (In coordination with the NGI-Manager):
  - NGI-Security Officer should be able and have the mandate to enforce policies (EGI and NGI) ex: that sites respond/react in a timely manner.
  - response times, as stated in the Incident-Response-Procedure (respond within 4 working hours)
  - be able to do analysis of any grid security issue in your country.
  - install updates in case of vulnerabilities according to the recommendations of EGI-CSIRT.
- NGI-Security Officer should be able and have the mandate to suspend a site in his/her country as a last resort.

# EGI-CSIRT Group structure

- EGI-CSIRT will consist of more than 35 NGI-Security-Officers.
- Group based approach is used to coordinate the security activities in the project.
- Basis of the group structure are the OSCT activities which should be continued in EGI.
- Incident Response Task Force needs to be moderated.
- The supporting groups are not static, participation in multiple groups might be needed. Ex. localised security Monitoring, local Security Drills
- Since the problems using localised services might be similar in the NGIs, a focus will be on documentation.

# EGI-CSIRT Group structure



# EGI-CSIRT Groups

- Presentation of the OSCT activity coordinators.
- Kick-start the EGI-CSIRT groups.
- To keep you informed about the status of the Groups please indicate to which groups you want to contribute.