Table of Contents

This page is obsolete!

For up to dated information about EGI CSIRT please check EGI CSIRT wiki page at: https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page

The EGI Computer Security and Incident Response Team - EGI CSIRT

[quoted from section TSA1.2: A Secure Infrastructure of EGI-InSPIRE proposal]

The EGI CSIRT covers all aspects of operational security aimed at achieving a 'secure infrastructure' within EGI and relies on site and NGI security contact information maintained in the GOCDB by each NGI. The EGI CSIRT ensures both the coordination with peer grids and with the NGIs and NREN CSIRTs. The EGI CSIRT acts as a forum to combine efforts and resources from the NGIs in different areas, including Grid security monitoring, Security training and dissemination, and improvements in responses to incidents (e.g. security drills). Each NGI will appoint an NGI Security Officer in order to provide the NGI CSIRT function. The resulting group of NGI Security Officers collaborate as part of the EGI CSIRT.

The EGI CSIRT is led and coordinated by the EGI Security Officer, whose role and mission are defined by security policies approved by EGI and the NGIs.

Requested Effort (as specified in EGI-InSPIRE proposal): 335 PM (person/month) over 4 years period (83.75PM/year)

4PMs UPT	12PMs UNI LINZ	16PMs IPP-BAS	16PMs SWITCH	12PMs CESNET	20PMs KIT	4PMs UCPH
16PMs CSIC	3PMs CSC	44PMs CNRS	4PMs GRNET	8PMs KFKI	8PMs TCD	4PMs IUCC
12PMs INFN	4PMs UoM	4PMs UKIM	28PMs NCF	8PMs SIGMA	12PMs CYFRONET	8PMs LIP
8PMs IPB	12PMs e-ARENA	8PMs VR SNIC	4PMs ARNES	8PMs UI SAV	8PMs TUBUTAK ULAKBIM	40PMs STFC

EGI-CSIRT Groups

The following working groups were proposed to be formed before the start of EGI project. Each group is coordinated by a group coordinator and consists of NGI security officers. A NGI security officer (as well as the other members of the NGI's security team) can join more than one group. A NGI security officer can also take one (but only one) group coordinator role. More groups will be formed when needed.

- Incident Response Task Force
- Security Monitoring Group
- Security Drills Group
- Training and dissemination group

As discussed at the face to face meeting on 22nd/23rd March 2010, a list of tasks were identified within each group. It is NOT a complete list and **input/suggestion** are highly appreciated. The to be appointed group coordinators might update or ammend the list of tasks when applicable.

Basic requirement of a group coordinator

A coordinator with sufficient experience will be appointed in each group to coordinate the work within the group.The coordinator should be able to:

- maintain and develop good working relationship with both group members, other CSIRT members and external colleagues;

- set clear and measurable objectives, tasks and milestones;
- coordinate all activities within the group to make sure that agreed objectives, tasks and milestones can be achieved;
- perform additional assignments and responsibilities as agreed with the EGI CSIRT security officer or the project management;

EGI CSIRT members (aka NGI security officers) are encouraged to take either a coordinator role or to participate into work of these groups.

NOTE: in order to get the team ready before 1st May, the deadline of group coordinator application (express your interest in the role) is Friday 16th April.

Incident Response Task Force (IRTF)

Objective: Handle day to day operational security issues and coordinate Computer-Security-Incident-Response across the EGI infrastructure.

Tasks:

- Replace OSCT-DC
- Swift response to any reported computer security incident affecting EGI infrastruture
- Security Incident Management
    - Existing communication channel (mail list/security wiki) migration
    - New communication channel (if needed) setup
    - Incident response tools development, evaluation and adaptation
    - Incident handling procedures update/maintainence
- Adapt the current EGEE computer security incident response procedures to EGI framework.
- Establish addtional operational and/or escalation procedures when required
    - a procedure to suspend a site from the EGI infrastructure
    - a procedure and agreed criteria to ban (blacklist) a user, a group of users and/or a VO
- vulnerability assessment
    - Regularly monitor vulnerability databases
    - Assess impact of vulnerabilities on the EGI infrastructure
    - Advise the project mitigation solutions

Additional requirement to the Coordinator: Ideally, the coordinator should have track record of coordinating computer security incident response across multiple Grids/countries.

Coordinator: TBC

Volunteers:

Name	NGI	Home Orgnazation	Effort Avalible (PM)
Leif Nixon		NDGF	
Ake Sandgren		NDGF HPC2N	
Daniel Kalici (for Malware Analysis)		NDGF	
Daniel Kouril		CESNET	
Michal Prochazka		CESNET	
Dorine Fouossong	France NGI		
David O'Callaghan	Irland NGI	TCD	
Mingchao Ma	UK NGI	STFC - RAL	
Christos Triantafyllidis	Greek NGI		
Ursula Epting	German NGI	KIT-GridKa	

Tobias Dussa	German NGI	KIT-GridKa	
Michael Hausding	Switzerland NGI	SWITCH	
Carlos Fuentes	Spanish NGI	RedIris	
Sven Gabriel	Dutch NGI	NIKHEF	
Nuno Dias	Portugal NGI	LIP	

Vulnerability assessment (part of incident response task force)

Name	NGI	Home Organization	Effort Available (PM)
Leif Nixon		NDGF	
Michael Hausding	Switzerland NGI	SWITCH	
Xander Jansen	Dutch NGI	SURFcert	
Detlev Matthies	German NGI	DFN	
Dorine Fouossong	France NGI		

Security Drills Group (SDG)

Objective: Provide an overview of the various CSIRTs readiness' to react to an computer security incident and challenge the inter CSIRT communcation channels.

Tasks:

- Design and set-up realistic simmulations of computer security incident scenarios.
    - Address various grid middleware components (ex: VO Job submission framework (SSC4))
    - Assess the capabilities/suitability of fabric management tools for operational security.
    - Assess security related software (managability) ex: glexec, central banning.
    - New tools for IRTF could first be tested here.
- Run/evaluate/disseminate the security drills on the project level.
- Collect the sites feedback, ex. which tools are needed to improve the response.
- Provide a framwork so that NGIs can run a particular security drill at some or all of their sites.
- Set up a "Sites-Readiness" web page were the results of the security drills are collected. Access restricted to EGI-CSIRT, IRTF, EGI/NGI Management.

Role of the coordinator: Coordinate the project wide runs with the various involved (VO) CSIRTs. Coordinate with the NGI Security Officers local runs in order to have a optimal coverage of the challenged sites and by this getting a map of the sites readiness to respond to an computer security incident.

Cooridiantor: TBC

Volunteers:

Name	NGI	Home Organization	Effort Available (PM)
Angela Poschlad	German NGI	KIT	
Detlev Matthies	German NGI	DFN	
Riccardo Brunetti	Italy NGI	INFN	
Guiseppe Misurelli	Italy NGI	INFN	
Sven Gabriel	Dutch NGI	NIKHEF	
Christos Triantafyllidis	Greek NGI		
Edgars Znots	Latvia NGI		
Bartlomiej Balcerek	Poland NGI		

Emir Imamagic	MD NGI		

Security Monitoring Group (SMG)

Objective: Develop, deploy and maintain security monitoring tools.

Tasks:

- Pakiti:
  - Further development
  - Monitor the result of central Pakiti server and raise alarm if necessary
  - Support NGIs in setting up a national Pakiti instance.
  - Improve support for non rpm based distributions.
- Tools to trace user activity.
- Nagios:
  - Further development
  - Security probes development and maintances
  - Deploy security probes within the existing Nagios framework
  - Support NGIs to intergate security probes into their local NGI Nagios framework
- Explore the possibility of using APEL data for security monitoring and security incident handling purpose
- Explore the possibility of creating a security monitoring dashboard to aggreate, consolidate and visualize monitoring results

Coordinator: TBC

Volunteers

Name	NGI	Home Organization	Effort Available (PM)
David O'Callaghan	Irland NGI	TCD	
Christos Triantafyllidis	Greek NGI		
Jinny Chien		ASGC	
Daniel Kouril	Czech Republic NGI	CESNET	
Michal Prochazka	Czech Republic NGI	CESNET	
Dusan Vudragovic	Serbia NGI	AEGIS	
Angela Poschlad	German NGI	KIT	
Bartlomiej Balcerek	Poland NGI		
Emir Imamagic	MD NGI		
Riccardo Brunetti	Italy NGI	INFN	
Guiseppe Misurelli	Italy NGI	INFN	
Dorine Fouossong	France NGI		
Feyza Eryol	TR NGI	TUBITAK-ULAKBIM	

Training and Dissemination Group (TDG)

Objective: Raise security awareness and improve security for system administrators by providing security training and best practice

Tasks:

- Plan and organize training events

- Collect and archive training materials used in past events.
- Support NGIs setting up local training events.
- Develop training material
- Setup and maintain EGI CSIRT public and interal website and wiki

Coordinator: TBC

Volunteers:

Name	NGI	Home Organisation	Effort Available (PM)
Angela Poschlad	German NGI	KIT	
Detlev Matthies	German NGI	DFN	
Dorine Fouossong	France NGI		
Jinny Chien		ASGC	

-- MingchaoMa - 07-Apr-2010

This topic: LCG > EGI_CSIRT
Topic revision: r17 - 2010-07-06 - unknown