EGEE Operational Security

Mingchao Ma, STFC – RAL, UK
GridPP Security Officer
UKI ROC Security Contact
Operational Security Coordination Team (OSCT)

ISGC 2009 Taipei, 21st April 2009

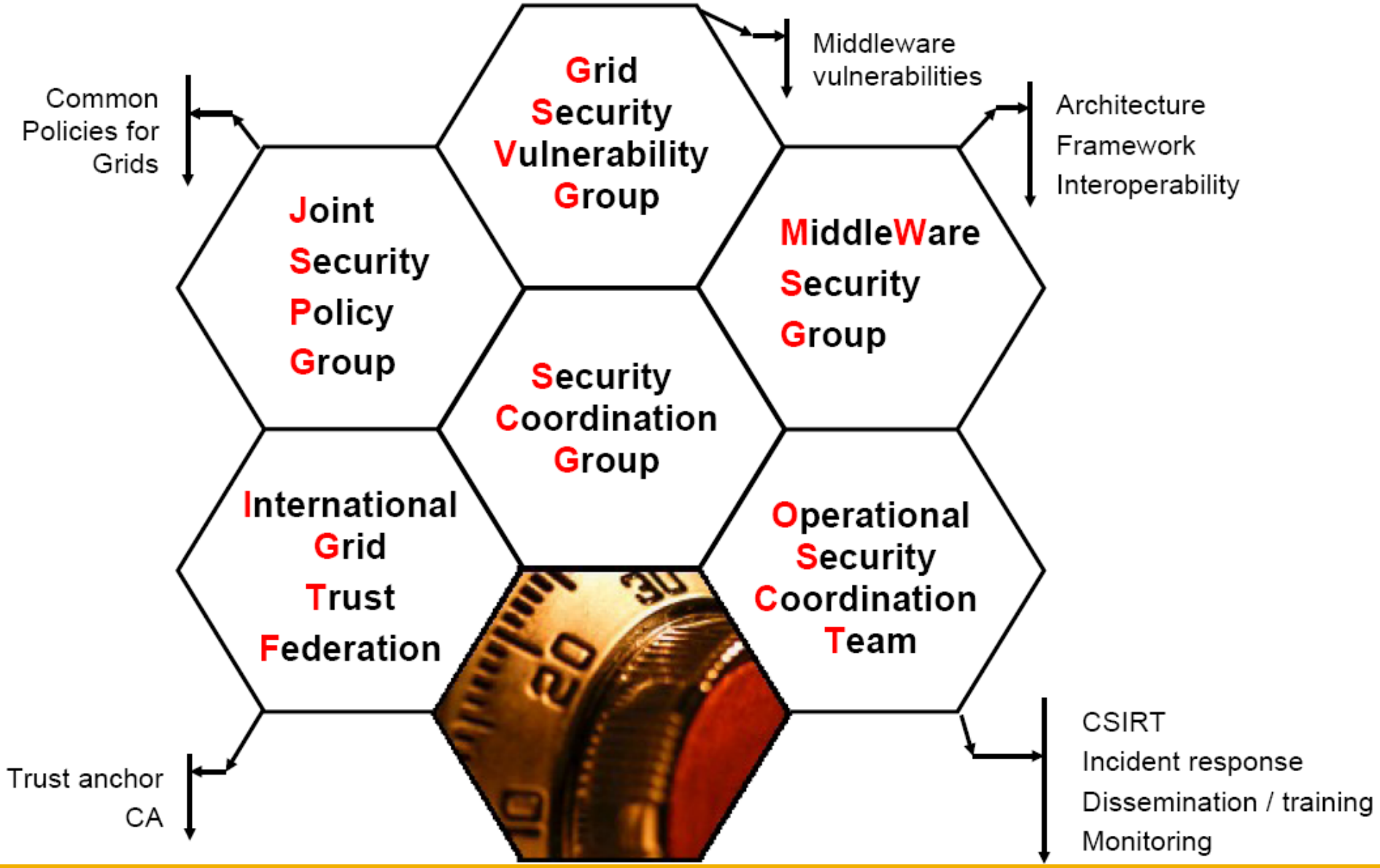
Science & Technology Facilities Council

Information Society and Media

Overview

- The EGEE Security Groups
- What is OSCT and Who are we?
- Current Activities
- Conclusion

EGEE Security Groups



OSCT

- The Operational Security Coordination Team (OSCT) provides an operational response to security threats against the EGEE infrastructure.
- It focuses mainly on computer security incidents handling, by providing reporting channels, pan-regional coordination and support.
- It also deals with security monitoring on the Grid and provides best practices and advice to Grid system administrators.

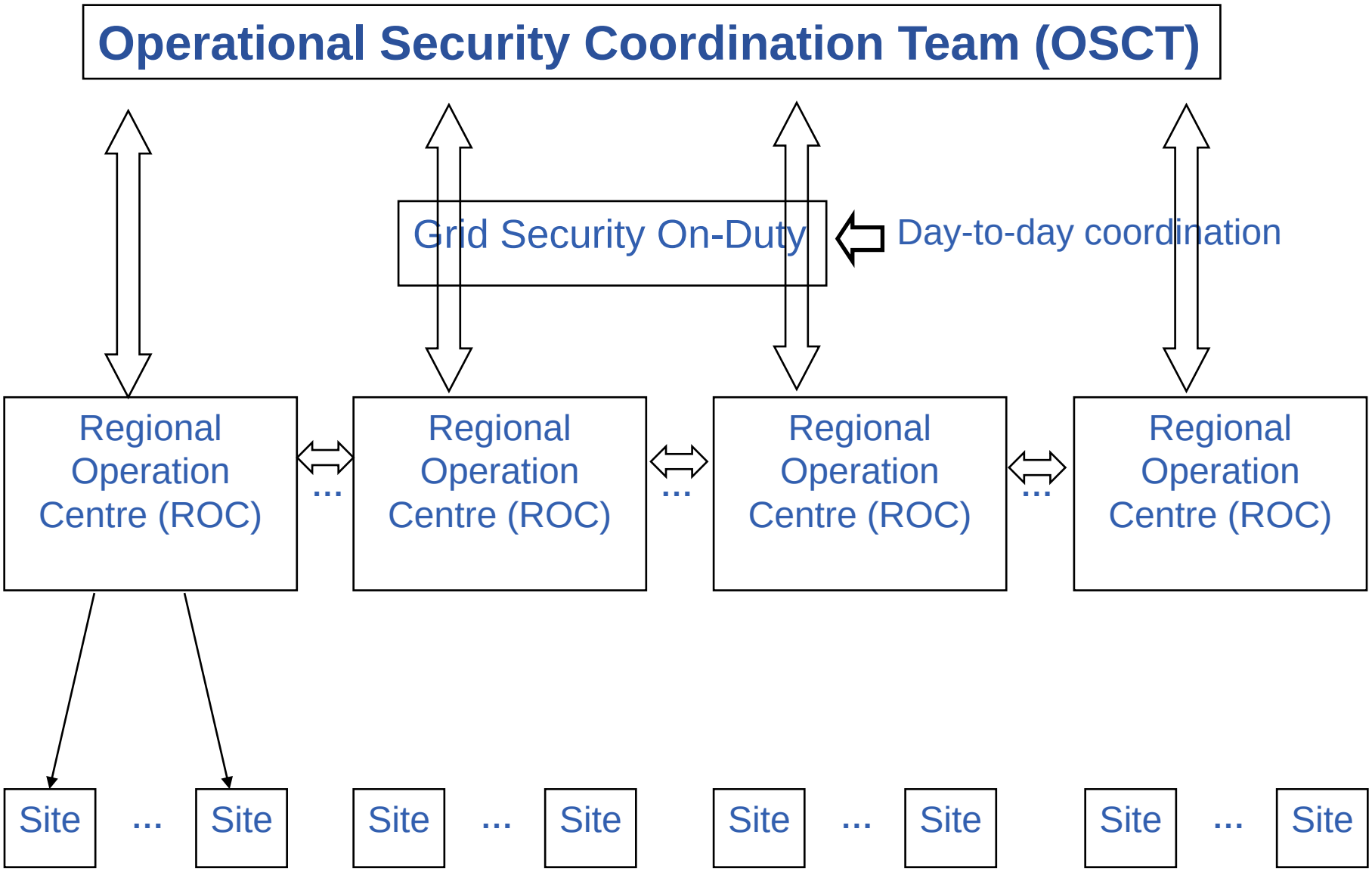
Members

- **The OSCT is led by the EGEE/LCG Security Officer and includes security contacts from each EGEE region, who provide support for daily security operations as part of an on-duty rota (OSCT-DC).**

- **11 federations (Regional Operation Centres-ROCs)**

  - AsiaPacific – AP ROC
  - Central Europe – CE ROC
  - CERN ROC
  - France – FR ROC
  - Germany and Switzerland – DECH
  - Italy – IT ROC
  - NorthEurope – NE ROC
  - SouthEast Europe – SEE ROC
  - SouthWest Europe – SWE ROC
  - United Kingdom and Ireland – UKI ROC
  - Russian – Russian ROC

OSCT Structure



OSCT Activities

- Weekly telephone meeting;
- Twice face-to-face meeting per year
- Work together with other security groups to improve Grid security;
- Analysing and evaluating security risks/vulnerabilities together with GSVG
- Provide security expertise to sites;
- Grid security incident handling;
- Security monitoring;
- Best practice, security training and dissemination

Incident Handling

- **Grid security incident handling**
  - Following Grid Security Policy and OSCT Incident Response Procedure;
  - OSCT-DC is responsible for coordinating the incident response with assistance of other OSCT members
    - Analyse available information and follow the most likely leads
    - Contact affected sites and other CSIRT teams for further information
    - Keep involved sites and partners updated of the progress
  - The objective is
    - To quickly identify and contain the incident from widely spreading;
    - To understand the incident: what, how, when, why and who;
    - To restore affected system/services and prevent re-occurrence;
  - Manage information flow among affected sites, EGEE sites, external partner sites (e.g. OSG and TG in USA) and/or NRENs CERT teams – a very challenging task;

Current Work on IR

- Revising OSCT incident response procedure, almost done!
  - Specify timeframe in each step
  - Change of email address for incident report
- Pan-region, cross grid and NRENs CSIRT IR channel
  - To share information
  - To keep information secure
- Security Service Challenges (SSC)
  - Like a fire drill
  - Tier1 sites are challenged by OSCT;
  - Tier2 sites are challenged by ROC security officer;
  - Familiarised with incident handling procedure;
  - Verify communication channels;
  - Improve incident handling at all levels;
  - SSC3 ongoing;

Security Monitoring

- **To raise & sustain overall security level**
  - Assist grid participants to keep their resources secure
    - Focusing on grid services
  - Primarily focusing on infrastructure, not applications
    - Self audit of sites (decreasing overhead)
  - Detect operational problems before they may lead to incidents
    - Notification of responsible people
  - If possible, detect known vulnerabilities and incidents
- **To assist in incident handling**
  - Analyze data gathered by monitoring (Pakiti history, …)
  - Analyze logs to trace users' activities
    - On-demand rather then general grid IDS
- **To increase awareness of sites, other groups, VOs**
  - Highlighting results of security probes
  - Existence of OSCT and its functions

Content from Daniel Kouril

Current Work on Monitoring

- **Integration with operations automation team (OAT)**
  - The OAT is developing a framework based on Nagios to check Grid functionality at different levels (e.g. ROC, site, VOs)
  - Replacement of SAM framework with Nagios-based framework
  - Collaborate with the OAT to integrate security tests
- **Risk analysis and tests design, development**
  - New security probes to cover the main risks identified
- **Pakiti – Patch management**
  - To check the patching status of Linux system
  - Can also be integrated into OAT Nagios framework
- **Log Analysis & Users Traceability**
  - Tools for various log analysis
  - Site/Node and Grid (VO) level
    - Syslog handling, L&B utilization

Training and Dissemination

- **Document and encourage adoption of best practice**
  - Gather security-related information from various sources;
  - Security RSS feed;
  - OSCT website/Wiki;
  - Security page including various topics/links on OSCT website
  - gLite Service reference cards
    - Dedicated “Security information” section;
- **Security training workshops;**
  - For system managers and administrators;
  - Organised either by ROC security officers or OSCT;
- **To provide and share security expertise;**
- **To improve security awareness and skills;**
- **To improve all over security of the Grid;**

Service Reference Cards

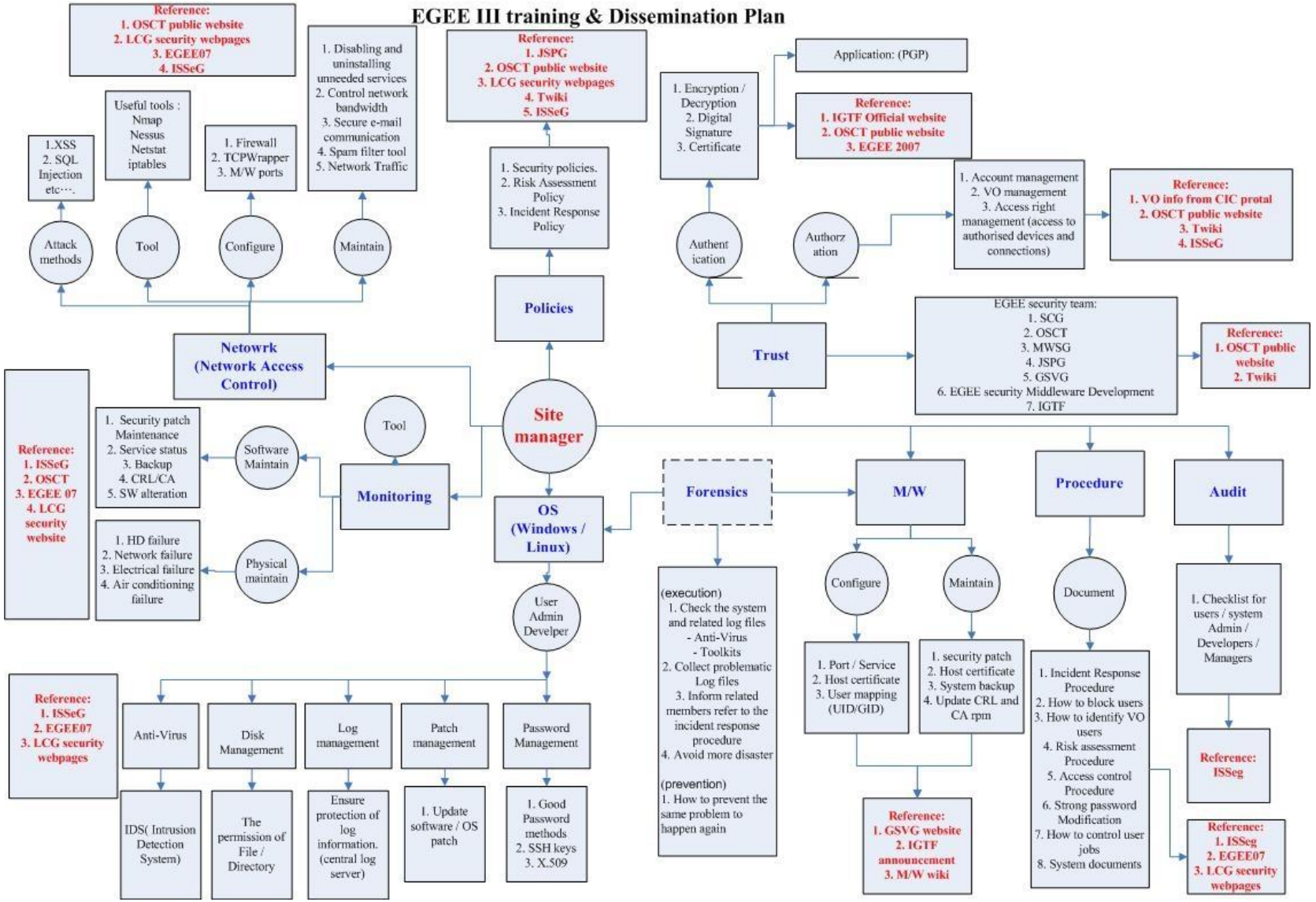
- **gLite Service reference cards**
  - https://twiki.cern.ch/twiki/bin/view/EGEE/ServiceReferenceCards

- gLite-AMGA - ARDA Metadata Catalog
- glite-BDII - Berkeley Database Information Index
- glite-CREAM_CE - gLite CREAM Computing Element
- glite-DPM - Disk Pool Manager
- glite-FTS - File Transfer Service
- glite-LFC - LCG File Catalog
- gLite-LB - Logging and Bookkeeping service
- glite-MON - Monitoring System Collector Server
- glite-PX - MyProxy server
- glite-UI - User Interface
- glite-VOBOX - Virtual Organisation Node
- glite-VOMS - Virtual Organisation Membership System
- gLite-WMS - Workload Management Service
- glite-WN - Worker Node
- lcg-CE - LCG Computing Elements

Service reference cards

- **Each service card has a “security information” section**
  - Access control Mechanism description (authentication & authorization)
  - How to block/ban a user
  - Network Usage
  - Firewall configuration
  - Security recommendations
  - Security incompatibilities
  - List of externals (packages are NOT maintained by Red Hat or by gLite)
  - Other security relevant comments
- **Working in progress**

Security Page



Security Page

- **Still in very early stage, will be hosted at OSCT website**
- **Topics cover**
  - Security policies, procedures
  - Security monitoring
  - Middleware security
  - OS security
  - Network security
  - Trust (CA, PKI and IGTF)
  - Forensics
  - … …

Training

- **Security training**
  - Target system managers and administrators, NOT end users;
  - No dedicated budget for security training;
  - Incorporate training into other conferences/events;

  Past training events
  - EGEE'07, 1st -5th October 2007, Budapest
  - EGEE'08, 22nd -26th September 2008, Istanbul
  - Security training at Laboratory APC, France, 2nd -3rd April 2009
  - Security training at ISGC 2009, Taipei, 19th April 2009

  Upcoming training events
  - Security training workshop at RAL, UK, 1st July, 2009
  - GridKa School at Karlsruhe, Germany 31st Aug.- 4th Sep. 2009
  - EGEE'09, 21-25 September 2009, Barcelona
  - Some ROCs are planing trainings in their regions as well

Conclusion

- **Handling Grid incident requires a lot of communication**
  - Communication is the key;
  - Managing information flow across Grid and external partners is a very challenging task;
- **Training and dissemination requires significant efforts**
  - Grid software are too complex;
  - Grid software are constantly changing;
  - Staff has various level of skills;
  - Very limited budget and manpower;
- **To be able to monitor the Grid at various levels is very important, a lot of work need to be done;**
  - Complex infrastructure
  - Security vs. privacy

Links and Support Contacts

EGEE Security

http://www.eu-egee.org/security/

OSCT website and Wiki

http://osct.web.cern.ch/osct/

https://twiki.cern.ch/twiki/bin/view/LCG/OSCT

Vulnerability reporting

- grid-vulnerability-report@cern.ch

Incident reporting

- project-egee-security-csirts@in2p3.fr
- project-egee-security-contacts@in2p3.fr
- Incident response procedure
  - https://edms.cern.ch/document/867454/

More Links

Security RSS feed:

http://rss-grid-security.cern.ch/rss.php

Pakiti: http://sourceforge.net/projects/pakiti/

OAT Framework:

https://twiki.cern.ch/twiki/bin/view/EGEE/MultiLevelMonitoringOverview

Joint Security Policy Group (JSPG): http://www.jspg.org/

Discussion