TSA 1.4 Operational Security

Romain Wartel
CERN, IT Department
EGEE Operational Security Coordination Team

EGEE'09, Barcelona, Spain, 21-25 September 2009

www.eu-egee.org

OSCT - security monitoring

- **Different activities**
  - Dedicated tools (mainly logging and traceability)
  - Integration of security tests as part of the OAT framework
  - Close collaboration with the OAT

- **Pakiti**
  - Tracking the patching status of sites
  - Development slower than expected, stable release “soon”
  - Extremely useful

Pakiti Package Results for CVE-2009-2698

CVE: **CVE-2009-2698** - Click to select other CVE

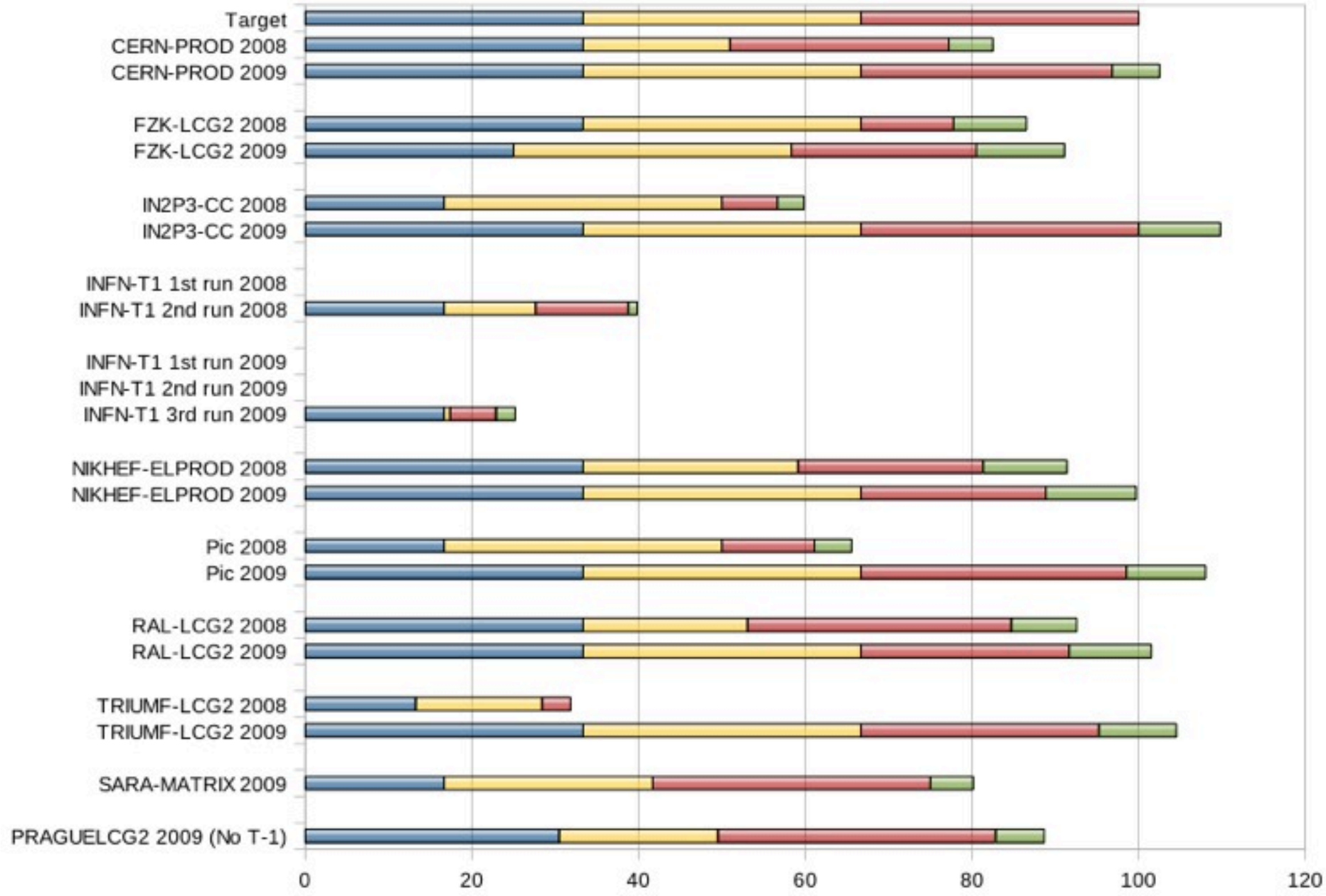
Domain: All

You can also select hosts by: CVEs Packages

Domain Host	Packages	Last report
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	16 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	15 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	15 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	16 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	15 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	15 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	16 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	16 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	15 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	17 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	17 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	15 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	17 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	17 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	15 September 2009
[redacted]	kernel-smp (0:2.6.9-78.0.8.EL)	17 September 2009

OSCT - Security Challenges

- **Final results of the 2009 campaign**



- **SSC campaigns completed also in the ROCs**

OSCT - incident response

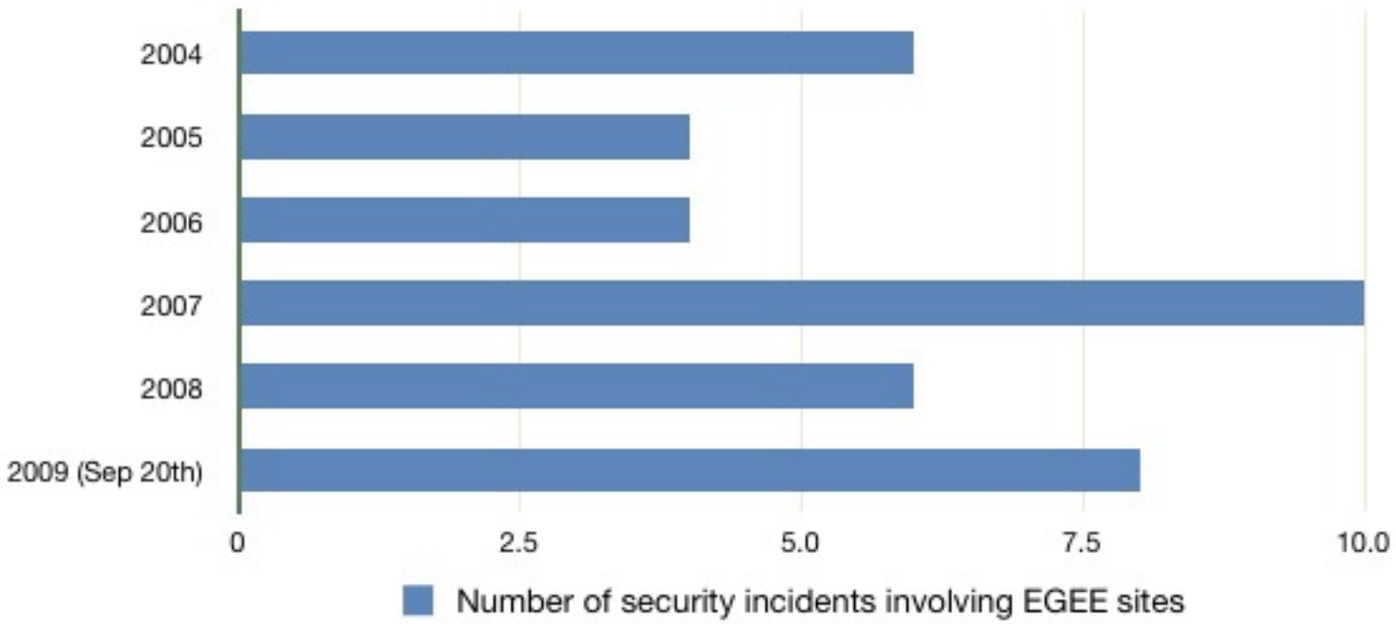
- **Update incident response procedure**
  - Redesigned to include feedback and metrics from SSC
  - Specific details and contact points added
    - User suspension (exposed, compromised certificate)
    - Contact with the VOs, CAs and external organisations added
    - What information is expected from the sites
    - Where to find the information usually needed
    - Unique incident identifier usage
  - Templates for initial reporting and final report
  - Coordination process within the OSCT described

https://edms.cern.ch/file/867454/2/EGEE_Incident_Response_Procedure.pdf

http://cern.ch/osct/incident-reporting.html

OSCT - incident response

- **EGEE statistics on security incidents**



- **Common attack:**
  - Stolen SSH account(s), or Web application (known) vulnerability
  - Escalate as root (CVE-2009-2692, CVE-2009-2698, etc.)
  - Deploy rootkit or further malware
- **Several incidents avoidable if sites were up-to-date with security patches**

OSCT - security training

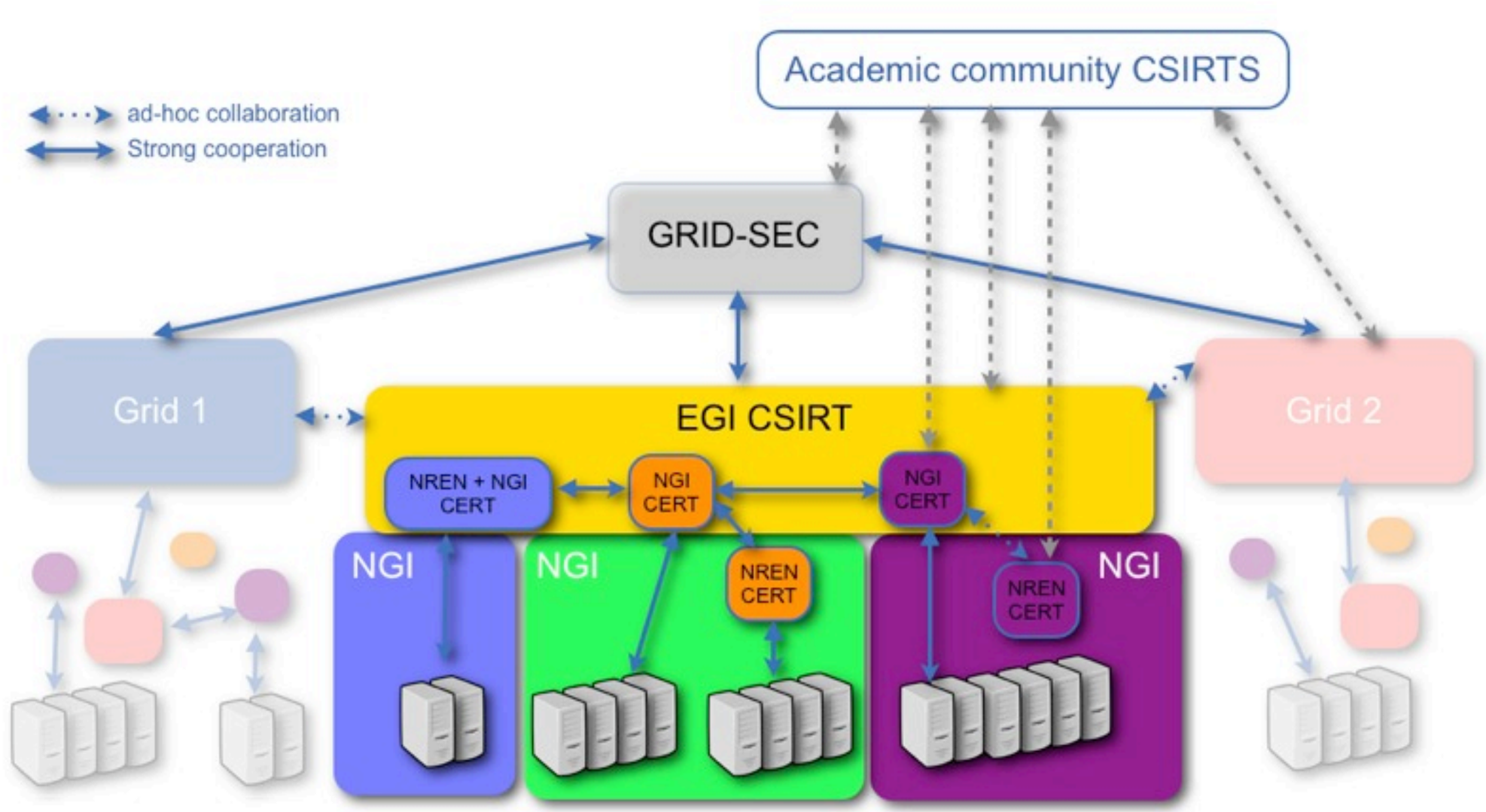
- **Main event organised this week**
  - http://indico.cern.ch/sessionDisplay.py?sessionId=26&slotId=0&confId=55893
- **Several localised events organised in the regions**
- **Last major training event organised at ISGC09**
  - http://event.twgrid.org/isgc2009/program.htm#gridtutorial
- **Information added to the gLite reference cards**
  - https://twiki.cern.ch/twiki/bin/view/EGEE/ServiceReferenceCards
- **New training and dissemination website being designed**

OSCT - external collaboration

- **Collaboration with the NRENs**
  - Significant progress since last year
  - Many more contacts established between the ROCs and their NRENs
  - BoF at TERENA 09
  - Collaboration plan agreed, implementation in progress
  - As far as we can go, the rest is in the hands of each ROC/NREN
- **Collaboration with peer grids**
  - Creation of GRID-SEC
    - "A coordinated response to cross-grid security incidents"
    - http://cern.ch/grid-sec/
  - Framework to share incident-related information
  - Rather extensive coverage of the academic community
  - Already been handling 2 cross-grid security incidents
    - Incidents affecting sites belonging to different grids

Towards EGI

- **Transforming the EGEE OSCT in an EGI CSIRT**
  - Approach the NREN CERTs community (TF-CSIRT)
  - Establish the relevant structure, communication channels
  - Very similar to the current model



Joint Security Policy Group

- **Five recently approved and adopted policies:**
  - **Virtual Organisation Registration Security Policy**
    https://edms.cern.ch/document/573348/8
  - **Virtual Organisation Membership Management Policy**
    https://edms.cern.ch/document/428034/3
  - **Grid Policy on the Handling of User-Level Job Accounting Data**
    https://edms.cern.ch/document/855382/5
  - **VO Portal Policy**
    https://edms.cern.ch/document/972973/6
  - **Security Incident Response Policy**
    https://edms.cern.ch/document/428035/7
- **Current revisions (**http://www.jspg.org/wiki/)
  - Site Registration Security Policy
    - Remove EGEE-specific procedures and unify style
  - Grid AUP
    - Some Grids use it but have modified our text
- **Some infrastructures do not have VOs**

Security Policy – EGI transition

- **JSPG now working on new Security Policy Framework**
- **Goals:**
  - Enable interoperation of collaborating Grids (in EGI era)
    - aimed at managing cross-grid operational security risks
  - Identify policy components to help trust building between Grids
- **Not imposing a single policy for all**
  - But grids can use JSPG policies if they wish
  - Present the current set of JSPG policies
  - Taking high-level view to identify those necessary components
- **During next few months**
  - Finalise the draft framework & ensure nothing is missing
- **Then before end of EGEE-III**
  - Create generic description of the policy components
- **More details in Dave Kelsey's talk (Monday afternoon)**

Grid Software Vulnerabilities

- **174 Issues submitted since started in 2005**
  - (28 submitted in last 12 months)
  - Since mid 2006: 1EC, 19 High, 21 Moderate, 39 Low
- **Goal: identify and manage middleware vulnerabilities**
  - Important service for any software provider
  - Important for the middleware to be used by EGI too
  - Responsible disclosure: some independence from the software development/release process needed
- **Any UMD/EGI software provider would agree to:**
  - The responsible disclosure strategy
  - Handle the vulnerability affecting their component
  - A response time for this handling process
  - Follow the EGI security release cycle strategy
- **A lot of the details still need to be agreed**

Trust fabric

- **EUGridPMA and IGTF**
  - The European Policy Management Authority for Grid Authentication in e-Science
  - Establish requirements and best practices for grid identity providers
  - Enable a common trust domain applicable to authentication of end-entities
  - Mature and successful collaborative distributed activity