

# Security Monitoring in EGEE

*Daniel Kouřil, CESNET, kouril@ics.muni.cz*  
*EGEE09 Conference*

- **Detecting operational problems or even incidents**
- **Help sites to keep their resources secure**
  - Warning sites exposing vulnerabilities
- **Only a basic set of probes currently**
- **Main focus on higher levels (ROC, project)**
  - Provide the project and ROC (OSCT) with information about site status
  - not concerned with site level
- **No special privileges required from sites**
  - Only public interfaces used
- **<https://twiki.cern.ch/twiki/pub/LCG/OSCT-EGEEIII-tasks/security-monitoring-v0.12.pdf>**

- **A few SAM tests used**
  - CRL, file permission checks, Pakiti (patching status)
  - Results encrypted and only available to ROC security contacts
- **Further focus on Nagios-based framework**
  - Project and ROC view
    - SAM probes ported
    - Tests to be launched from ROC-level Nagios
  - Results collected in a standard way via message bus
    - Encryption must be applied – under discussion
  - Access allowed to ROC security contacts and site admins
    - Synchronized with GOC DB
  - Hopefully new probes will be developed
- **Check also poster #25**

- **Open source tool to check patching status**
  - <https://www.sf.net/projects/pakiti>
  - Any site can run its own Pakiti server to monitor internal machines
- **Server evaluates packages installed on clients**
  - Detects security patches not applied
  - Allows for searching for particular vulnerabilities (CVE)
    - Proved very useful recently (CVE-2009-2692, CVE-2009-2698)
- **Currently maintained by OSCT**
  - A lot of improvements applied recently
  - New version designed and prototyped during summer
- **OSCT operates Pakiti server for EGEE**
  - Information collected with SAM/Nagios probes (WNs)
  - Only OSCT members allowed to access

