Security Monitoring

Daniel Kouril, kouril@ics.muni.cz

EGEE09 Conference

EGEE and gLite are registered trademarks

The Activity

- **Detect operational problems before they may lead to incidents**
  - Focus on grid services, not OS level
- **Primarily focusing on infrastructure, not applications/sites**
- **Assist in incident resolution**
  - Analyze logs to trace users'
- **Team established and working**
  - Daniel Kouřil, Michal Prochazka (CE), Riccardo Brunetti, Giuseppe Misurelli (Italy), Dorine Fouossong (France), Christos Triantafyllidis, (SEE), Eygene Ryabinkin (Russia)
- **Poster delivered**

Security Monitoring

- **Focus on infrastructure**
  - Not concerned with sites
  - Using „public“ interfaces, no special privileges needed
- **SAM tests still used in production**
  - CRLs, file permissions, Pakiti
- **Nagios utilization in progress**
  - Design document produced (see OSCT wiki)
  - SAM security probes ported/developed
  - Protection of results not addressed yet
    - Access control on Nagios implemented (based on GOC DB)
    - Encryption not solved – multiple ways/teams to present results
  - Discussions with OAT ongoing

Pakiti

- **Pakiti server**
  - https://pakiti.cern.ch/pakiti/
  - Data collected by production SAM probes (4500 hosts)
  - Any OSCT member can ask for access
  - Check the results and talk to sites – avoid miscomunications (PMB)
- **Maintanence, development**
  - New version prototyped
- **Sites installation possible**
  - New release will be published at Sourceforge, soon
- **Metrics for proper evaluations missing**
  - Many vulnerable packages don‘t harm often

Users‘ traceability

- **Processing of monitoring data to trace particular users**
- **Site and Grid (VO) level**
  - (Sys)log handling, L&B utilization
  - Different roles/privileges needed
- **Two tools developed so far for**
  - lcgCE for site admins
  - L&B for VO managers
- **First releases available**
  - See Guiseppe‘s talk at trainining session

Plans for EGEE III

- **Full integration with Nagios**
  - Sort out data protection issues
- **Ongoing Pakiti maintance**
  - Metrics (labeling)
- **Users‘ traceability**
  - Processing of old data from L&B (Job Provenance)
  - CREAM/BLAH support (?)
  - Promoting utilization of remote syslog
- **New security tests**
  - Phalanx2 detection, risk analysis (?)

- **Security monitoring must be addressed/provided**
  - Finish/maintain tools developed
  - Results evaluation
  - Focus on sites internals as well (?)

  ….
- **No sufficient resources on egi.eu level**
- **Collaboration among NGIs ?**