Enabling Grids for E-sciencE

Security Monitoring

Romain Wartel
Operational Security Coordination Team
OSCT-3 , Edinburgh
19/20 June 2007

www.eu-egee.org

Security Monitoring – Strategy

- Monitoring activity:
  - Design and implement security tests
  - Monitor the test (or alarms?)

  Who should do this? OSCT-DC? COD?
  - Send tickets to the site

- Tools and monitoring infrastructure
  - Nagios (Any feedback from UKI/DECH?)

  Should we put effort in this now?
  - Service availability monitoring (SAM)
  - Any additional suggestion?

Security Monitoring – SAM

- Requirements
  - The tests should run at all the sites
  - Their results must not be available in plain text
  - Their results must not be publicly visible on SAM/Gridview

- Changes to SAM
  - SAM and Gridview have been modified to handle encrypted test results
  - A sample security test has been created (based SFT-crl)

Security Monitoring – SAM

- Short term plans (Eduard Pauna – CERN/Openlab)
  - Design and implement more tests
  - Document the process to create/amend the security tests
  - Discuss with the SAM team how to integrate the security tests in the framework/portals
  - Understand how advanced can the tests be and how fast a new test can be added (ex: mitigating 0-day exploits)

- Proposed middle term plan (6 months)
  - All ROCs discuss what parameters should be monitored
  - Other ROCs contribute to advise, design/implement new tests
  - First alerts based on the results are used to raise tickets
  - Sites are contacted (using GGUS?)

- Proposed long term plan (>6 months)
  - OSCT-DC implements new tests based on needs?
  - Alarms are weighted and handled either via COD or OSCT-DC