Contribution ID: **256** Type: **Poster**

EGI Security Monitoring integration into the Operations Portal

Tuesday, May 22, 2012 1:30 PM (4h 45m)

The Operations Portal is a central service being used to support operations in the European Grid Infrastructure: a collaboration of National Grid Initiatives (NGIs) and several European International Research Organizations (EIROs). The EGI Operation Portal is providing a single access point to operational information gathered from various sources such as site topology database, monitoring systems, user support helpdesk, grid information system, VO database and VOMS servers etc.

Significant development effort has been put in place to implement synoptic view. The single operations platform has been proved invaluable for those who involve EGI operations such as site administrators, NGI representatives, VO managers and NGI operators.

In parallel with this work, over the years, the EGI CSIRT (Computer Security Incident Response Team) has been developing security monitoring tools to monitor the infrastructure and to alert resource providers on any identified security problem. Due to the large and increasing number of resources joining the EGI e-Infrastructure it becomes more and more challenging for the EGI CSIRT to follow up all identified security issues.

In order to scale up the operation capability a security dashboard has been developed. The security dashboard integrates into the EGI Operations Portal as a module which allows resource providers' security officers and its NGI operation staff to access the monitoring results, and therefore to handle the issues directly. The dashboard aggregates the data produced by different security monitoring components and provides interfaces to its visualization. Access to the collected data is subject to strict access control so that sensitive information is accessed in a controlled manner. The integration will also allow operational security issue handling workflow to be easily incorporated into existing issue handling procedure, thus significantly reduces overall operational cost.

The paper will first briefly introduce current security monitoring framework
and its key components : Nagios and Pakiti, followed by the detail design and implementation of the security dashboard. we will also present some early experience gained with regular utilization of the security dashboard and results that have improved security of the whole environment recently.

Primary authors: L'ORPHELIN, Cyril (CNRS/IN2P3); KOURIL, Daniel (Unknown); Dr MA, Mingchao (STFC - Rutherford Appleton Laboratory)

Presenters: L'ORPHELIN, Cyril (CNRS/IN2P3); KOURIL, Daniel (Unknown); Dr MA, Mingchao (STFC - Rutherford Appleton Laboratory)

Session Classification: Poster Session

Track Classification: Distributed Processing and Analysis on Grids and Clouds (track 3)