Working Group on Operational Security

Grid Operations and Fabric Workshop – CERN 2-4 November 2004

http://agenda.cern.ch/fullAgenda.php?ida=a044377

Chair: Ian Neilson. (ian.neilson@cern.ch)

It is hoped that the working group will have a workshop format to progress initiatives on operational grid security. Attendees are invited to actively participate in formulating a strategy for this area for the next 12 months. 2 principal areas are proposed for discussion: incident handling procedures and service challenges. What follows outlines some of the many questions that need to be answered in this activity which can be addressed by this working group. Further comments are welcome to the chair.

Acronyms:

JSPG – Joint Security Policy Group. EGEE+LCG Security Policy and Operations group with representation from Open Science Grid (OSG).

MWSG – Middleware Security Group. Wide representation run by EGEE/JRA3 including applications, EGEE/SA1, JSPG. Formulating middleware security requirements.

Incident Handling

The JSPG proposes that Operational Security for EGEE/LCG be coordinated through the formation of an Operational Security Coordination Team (OSCT). It is further proposed that the structure and requirements on this team and the associated incident handling procedures be based on the requirements derived from the OSG (draft) document Secuirty Incident Handling and Response available here: http://computing.fnal.gov/docdb/osg_documents//Static/Lists//FullList.html. The adoption of a common approach to incident handling between grid infrastructure operations is seen as highly beneficial.

Selected summary derived from this draft document at present are:

- Definition of grid incident
  - What are the boundaries between a grid incident and
- Requirements on reporting and responding to incidents
  - "Participating sites MUST…."
- Guidance on the sharing of data
- Organisational structures defined
  - Site contacts, technical & response experts, ad hoc teams, Security Operations Centres (SOC), advisory group, cross SOC for inter grid communications
- Supporting resources
  - Site contacts, site CSIRT lists, tracking, communication channels
- Process
  - Discovery, reporting, triage, containment, analysis, escalation etc.

- Relationship to other bodies
  - NRENs, CSIRTS, Press & media

Suggested topics for discussion at this workshop:

- Site Contacts data
  - Maintenance and management
    Links with site registration process, how are bona fide contacts established and maintained?
- Variance in site support availability
  - Is this and issue? How do we handle it?
    - Need to quantify and gather information
    - Establishing ‘support’ channel for ‘smaller’ sites if necessary?
- Relationship to NRENS/CSIRTS
  - What is available and appropriate? How does this vary?
- Establishing ad hoc teams, contacting experts
  - What are appropriate models for doing this?
- OSG Incident Handling Process
  - Comments? (See also MWSG/JRA3 draft doc: https://edms.cern.ch/document/501422)
- Press and media
  - What is needed?
- Security monitoring
  - What can be done?

Security Service Challenge

Critical to effective response will be having the necessary trace data available. Existing LCG Audit Requirements on sites (available here: http://proj-lcg-security.web.cern.ch/proj-lcg-security/documents.html) are in need of updating. The JSPG has proposed some simplistic ‘challenges’ to test the traceability of jobs and storage items (available here: https://edms.cern.ch/file/478367/0.2/2004_Challenge_Plan.pdf). Running these (or any) challenge gives opportunity to build OSCT and processes discussed above.

- How can these initial challenges be co-ordinated?
- What else might be appropriate?