Operational Security Working Group Topics

- Incident Handling Process
  - OSG Document Review & Comments: http://computing.fnal.gov/docdb/osg_documents//Static/Lists//FullList.html
  - MWSG/JRA3 doc: https://edms.cern.ch/document/501422
  - Relationship to existing local Incident Response procedures
- Variance in site support availability
  - How do we handle it?
    - Need to quantify and gather information. How?
    - Establishing 'support' channel for 'smaller' sites if necessary?
- Reporting channels
  - Relationship to / use of NRENS/CSIRTS. Regional variations?
  - Bridges to other grids (e.g. OSG)
  - Information disclosure/privacy concerns
  - Technology - Tracking system/lists. What is available and appropriate?
- Contacts data
  - Registry maintenance and management
  - Links with site registration process, how are bona fide contacts established and maintained?
- Establishing ad hoc teams, contacting experts
  - What are appropriate models for doing this?
- Press and media
  - What is needed?
- Security monitoring
  - What can be done?
- Service Challenges
  - What,who,how,when?

Operational Security Actions 1

- Aim: Move to functional operational security infrastructure conformant to agreed Policy. ASAP, Spring 2005
- Incident Handling Policy Agreement: OSG Doc
  - Input to Incident Handling Guide (in analysis area): Now, ALL
    - Should try to resolve conflict of need to restore service with benefit of analysis
- Form OSCT from (initially) ROC Security Contacts
  - ACTION: Security Officer & ROC managers, NOW
- Ticket tracking service investigations and setup
  - Can anything existing in project be used?
  - Basic proposal by end 2005: ACTION: Romain/OSCT ++?
- Security “Monitoring”
  - Simple & Proactive – ACTION: OSCT group/ Miguel to coordintate, begin now
- Contact data to be managed by regional contact ?in GOCdb
  - Extended by quantifying support level and local procedures
  - Action: OSCT JSPG GOC
- Service Challenges
  - Ongoing and as described.
  - ACTION: OSCT

Operational Security Actions 2

- Small site issues (but not only) –
  - Policy interpretation “Best Practice & Guidelines” for security policy (help admins)
  - ACTION: OSCT & Operational Support
- X-grid bridge activity -
  - Trust building and privacy issues dominate (bilateral & policy based)
  - Heads-up to be distributed to ‘registered’ contacts of other grids
- NRENS/CSIRTS
  - Distinct grid ‘coordinating activity’ is needed
  - But local sites/regions to ensure NREN CSIRTS are in the loop. ACTION: OSCT
- Operations Groups should include
  - disaster recovery planning and service continuity plan against critical services
  - Improvement in information dissemination
  - Provide guidelines & optional simple notification template
- Ad-hoc teams formed from regional contact and registered contacts to other activities
  - Noted issue of how 24X7 is handled. Operations Group SLA & ?remote admin.
- Press Office?
  - EGEE project office to be involved / local site policy?