Open Science Grid

Security Incident Handling and Response Communications Plan

Doug Pearson

OSG Integration Workshop at UC

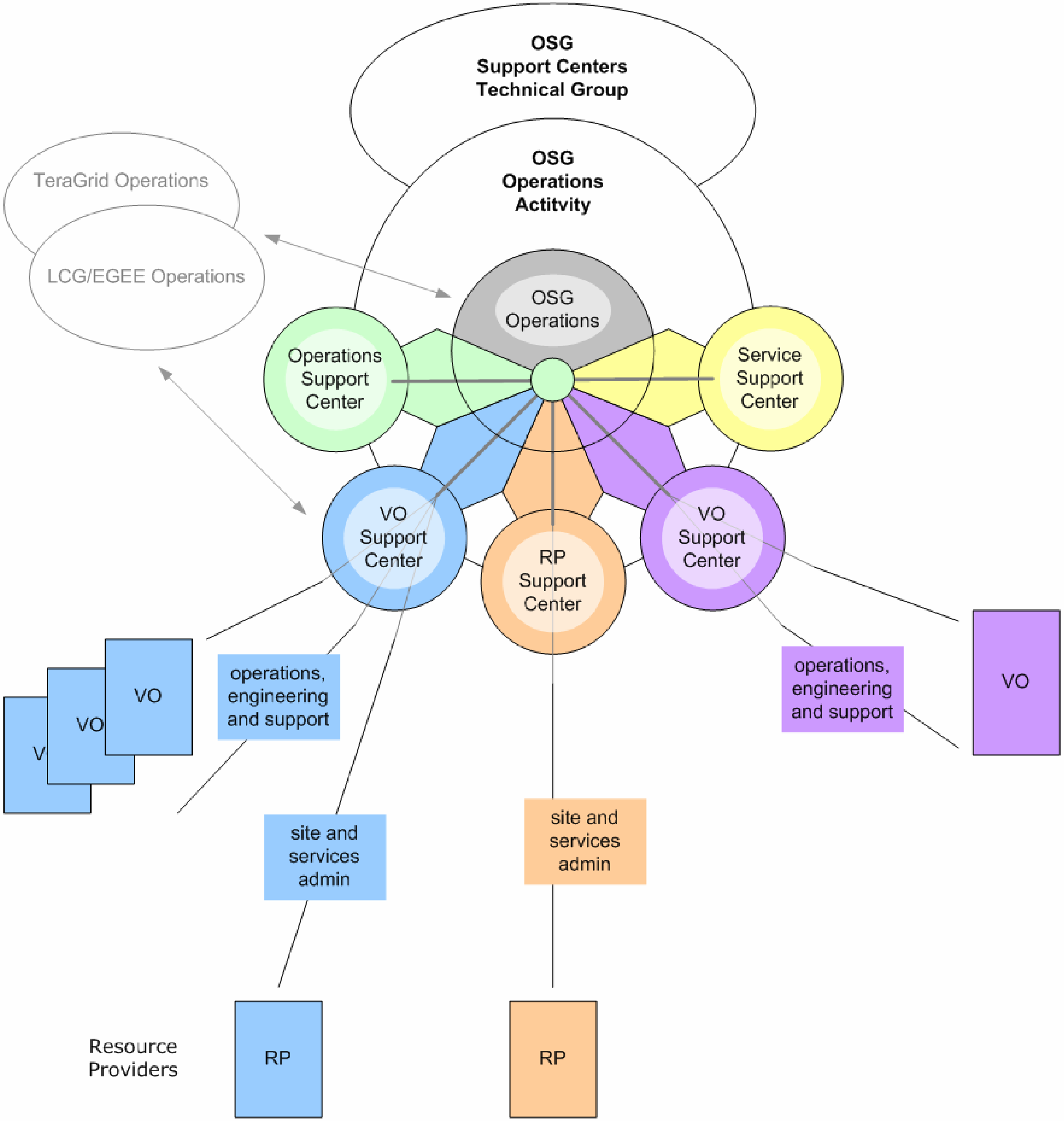
Feb 15-18, 2005

Service Description

- Provide a responsive and robust method to alert, report, and communicate regarding grid security incidents.

Background

- Operations Support Center
- goc@opensciencegrid.org
  - Mailing list that includes at minimum all the groups/sites that are providing “Operations Support Center” services



Open Science Grid

Components

- Registration
- Communications structure

Registration

- NOT finalized
- Is a subset of the general OSG new site registration
- Plan:
  - Site charter (or other?) describes required information and directions for submission, i.e. e-mail to goc@opensciencegrid.org
  - Operations Support Center updates appropriate mailing lists and welcomes new contacts to the list community.
  - Operations Support Center regularly queries each site and individuals to maintain list currency.

Communications

- incident-report-l@security.opensciencegrid.org
  - is a closed list comprising the grid security contacts for all grid participants and the grid operations center. Posting is restricted to list members. The list is intended solely for initial incident reporting, not for incident discussion. All email to this list is echoed onto the discussion list and replies are configured to be sent to the discussion list to keep traffic at a minimum.
- incident-discuss-l@security.opensciencegrid.org
  - is a closed list comprising the same members as INCIDENT-REPORT-L. The list is intended for discussion of reported incidents.

Communications

- Also the recommended:
  - abuse@opensciencegrid.org
  - security@opensciencegrid.org
    - These are routed to goc@opensciencegrid.org for review and forwarding as necessary to incident-report-l@security.opensciencegrid.org

Test and Validate

- Test registration (as it is) and incident handling:
  - New site joins the Grid; the process to register with the GOC is exercised, and GOC updates the security distribution lists.
  - Incident Discoverer-1 makes a report of Incident-1 by following the guidelines described in the OSG Security Incident Handling and Response Guide.
  - Incident Discoverer-2 makes a report of Incident-2 by using the security@opensciencegrid.org mailing address.
  - Sites react and respond according to the Guide.
  - Sites report post-mortem to TG-Security.

Support and Documentation

- OSG Security Incident Handling and Response Guide

Pending Issues and Next Steps

- General new site process – Site Charter or other?