OSG Cyber ~~Security~~ Health

OSG Site Administrators workshop
Indianapolis
August 6-7 2009

Doug Olson
dlolson@lbl.gov
LBNL

Agenda

- Welcome, introductions, agenda review (5 min)
- Security Risks – discussion (10 min)
- Site Responsibilities & Best Practices (45 min)
- Incident Response Forensics & Security Drill (30 min)
- Q&A on Tier 3 Issues (15 min)
- Certificate Handling (if time permits)

Security Risks

- https://twiki.grid.iu.edu/bin/view/Security/SecurityRisksCE?cover=print

Site Responsibilities

- https://twiki.grid.iu.edu/bin/view/Documentation/SecuritySiteResponsibilities?cover=print

Best Practices

https://twiki.grid.iu.edu/bin/view/Security/BestPractices

- Incident Handling & Forensics (See Anand's talk)
- Monitoring
  - discuss monitoring tools in use
  - monitoring ssh activity
- Logging
  - Can you find your log files?
  - Do you do central log collection (syslog, syslog-ng)?
- Updates
  - How often do you do OS updates?
  - How often to you do VDT updates?
- Firewalls
  - Do you use firewalls? What kind? What policies?
  - Are you familiar with globus & condor port ranges?

Incident Response Forensics & Security Drill

- Anand will describe security drill that was run earlier this year with the Tier 1 centers and cover the forensic techniques used to locate, remove and ban a “bad user”.

Q&A on Tier3 issues

- Open discussion on questions, issues, worries, … that Tier 3 site administrators have
- Bring your questions!

Certificate Handling

- Managing CA certificates
  - vdt-update-certs
    - vdt-control --enable vdt-update-certs
    - vdt-control --on vdt-update-certs
  - vdt-ca-manage
    - vdt-ca-manage setupca --location local --url osg
- Managing CRLs
  - Fetch-crl
- Example gridadmin certificate generation
  - cert-gridadmin –host your.univ.edu –service http …
- Setting up SMIME email
- …