Operational Security Coordination Team

OSCT report

EGEE-4, Pisa

Ian Neilson, CERN.

OSCT

- **Overview**
  - Security Service Challenge
    - Pal Anderssen
  - Security Monitoring
    - Romain Wartel
  - Incident Response
    - Ian Neilson

Security Service Challenges

- **Initial plan: simple, non-intrusive exercise**
  - Can we trace a job through the system?
    - Submit a job to a target site
    - Report the 'incident' to the target site's Security Contact
    - Trace credentials used, what/where, by what route?
- **SSC_1 targeting ROC sites completed in June 2005**
    - Nine sites provided debriefing information at the end of the campaign
    - All nine considered the exercise to have been useful and that the objectives had been met
    - A few sites reported that the execution had revealed shortfalls in the set-up at their sites
    - Three sites offered a HowTo recipe to track the job
    - An experienced team needs ~ 2 hours to extract the information
      - *An off-site Resource Broker complicates matter*

Security Service Challenges

- **Comments and questions raised at EGEE-4 OSCT session**
  - SSC should obey the normal rules of confidentiality
  - Transition to GGUS problem tracking tool
    - Is the required functionality available? TBD
  - Procedure for SSC reponse should be included into the operation (CIC and IRH)
  - Supplement the e-mail alert with telephone call early in the acknowledge phase of the challenge
  - Intrusive testing raises the issues of legal liability
    - *Might be permissible on non-production systems and with advance announcement*

Security Service Challenges

- **Future**
  - SSC_1 targeting regional sites from the ROCs
    - Scheduled for November 2005
  - SSC_2 affecting Storage Elements
    - Should use the same model: plain and simple
  - Other future SSC could be:
    - A given DN has accessed your site; what did it do and where?
    - ……
    - Patch test deployment
      - *should be integrated into the software deployment model, and not be treated in isolation as a SSC*

Grid Security Monitoring

- **Aim to provide tools to improve security**
- **Issues**
  - Policy
    - Who
  - Metrics
    - What
  - Infrastructure
    - How
- **Models**
  - *Mandatory*
    - *tests are grid jobs, with no specific privileges*
    - *tests are submitted to all the CEs, no exception*
    - *General results (failed, passed, warning) are public*
    - *detailed results are only available to a group of authenticated people*
  - *Subscription*
    - *tests are optional, sites have to ask for it*
    - *services passing the tests receive an extra "security label"*
    - *tests might sometimes require privileged access*
    - *detailed results only available to a group of authenticated people*

Grid Security Monitoring

- **Current status**
  - First test integrated into SFT framework
    - Monitoring last-download time for CRLs
    - Already turned up a ‘feature’ in download
    - Results displayed in OSCT presentation
- **Issues and Plans**
  - Interaction with GridVuln to extend (at least) SFT tests
  - SFTs are limited, subscription model needs to be worked on
  - Patch monitoring an important but complex issue
  - Difficult to monitor heterogeneous systems, we should prioritize

Incident Response Planning

- **Basic IR planning and model plans**
  - Proposed: *Incident Response Handbook*
    - Make procedures out of policy
      - *Quicker to update than policy*
      - *Lighter process than SSC*
    - Framework for planning activity
  - 4 Sections/Activities
    - Quick Start
      - *The basic process*
    - Grid resources
      - *References for contacts and administrators*
    - Services Reference
      - *Threat and impact by service*
    - Playbook
      - *Worked examples*

Incident Response Planning

- **Issues**
  - Not clear there is effort available now
  - Some dedicated resources in EGEE-II
  - Integration with operational procedures
    - CIC, GGUS ….
  - Operational role for OSCT
    - i.e. co-ordination during incident
  - Peering grid projects
  - NREN CSIRTS

Thank You