LCG/EGEE Security Service Challenge (SSC)

Pål S. Anderssen

CERN - IT

Security Service Challenges

- Announced ‘incident’ challenges
  - Check processes are understood
  - Check the information is available
  - Check communication lines
  - Provide a base-line for the improvement cycle
- 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?

Security Service Challenge level 1 (SSC_1)

- A very simple beta toolkit for a non-intrusive job
- Steps of the SSC_1:
  - The job is submitted to the target site
  - After ~20 hours ‘alert’ is sent to the target site’s Security Contact:
    - Indicating:
      - » UNIX-uid of job
      - » hostname of target
      - » the approximate time when job was active on target
    - Requesting:
      - » the Grid credentials used
      - » the IP-address of submitting UI
      - » the name of the executed binary
      - » the exact time of execution
- During the process, reporting and debriefing info is posted to the Savannah tracking tool

SSC_1 ROC Campaign, June 2005

Outline of results

- Ten EGEE Regional Operational Center sites were targeted
- Nine sites were able to accept job submission and execute the job
- Six sites reported within 1.5 working day
- Three ROCs needed a reminder before they responded
- There were seven satisfactory and two incomplete responses
- During the entire process, reporting and debriefing info has been posted to the Savannah problem tracking tool -

https://savannah.cern.ch/projects/lcg-ssc

SSC_1 ROC Campaign, June 2005

Debriefing report in brief

- 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
- The full report is available at –

http://grid-deployment.web.cern.ch/griddeployment/ssc/DebriefRecommend.txt

SSC_1 regional campaign, November 2005

- Job submission will be controlled by each region's ROC
- Following the recommendations from the June campaign, there are a few changes:
  - A group in Savannah has been configured for the benefit of ROCs which do not have problem tracking tool in place
  - All dates and times must be expressed in UTC
  - Proactive follow-up
    - The site security contacts are asked to acknowledge receipt of alert within one working day
    - Failing the deadline, a reminder will be sent
    - Failing a new one working day deadline, the site will be contacted by phone
    - Failing an over-all deadline of 5 working days, the site's response will be marked as incomplete

The future

- Guide-line and motivation for security challenges
  - *Start small and keep it simple*
  - Raise awareness and exercise communication channels
- Design criteria for the SSC “Storage Element” incident
- Challenge the Security Patch Deployment
  - Need quick response to security patch deployment calls
    - 24, 48 or 72 hours ?, your input is required
  - Site monitoring tools may help assess the deployment response times
- Potential issue: Confidentiality of information
- Un-announced challenges
- Disruptive/Intrusive testing – To be defined and approved
- The real thing –
    - operational experience