Operational Security update

Romain Wartel

GDB, 10th December 2008

EGEE and gLite are registered trademarks

Overall team strategy

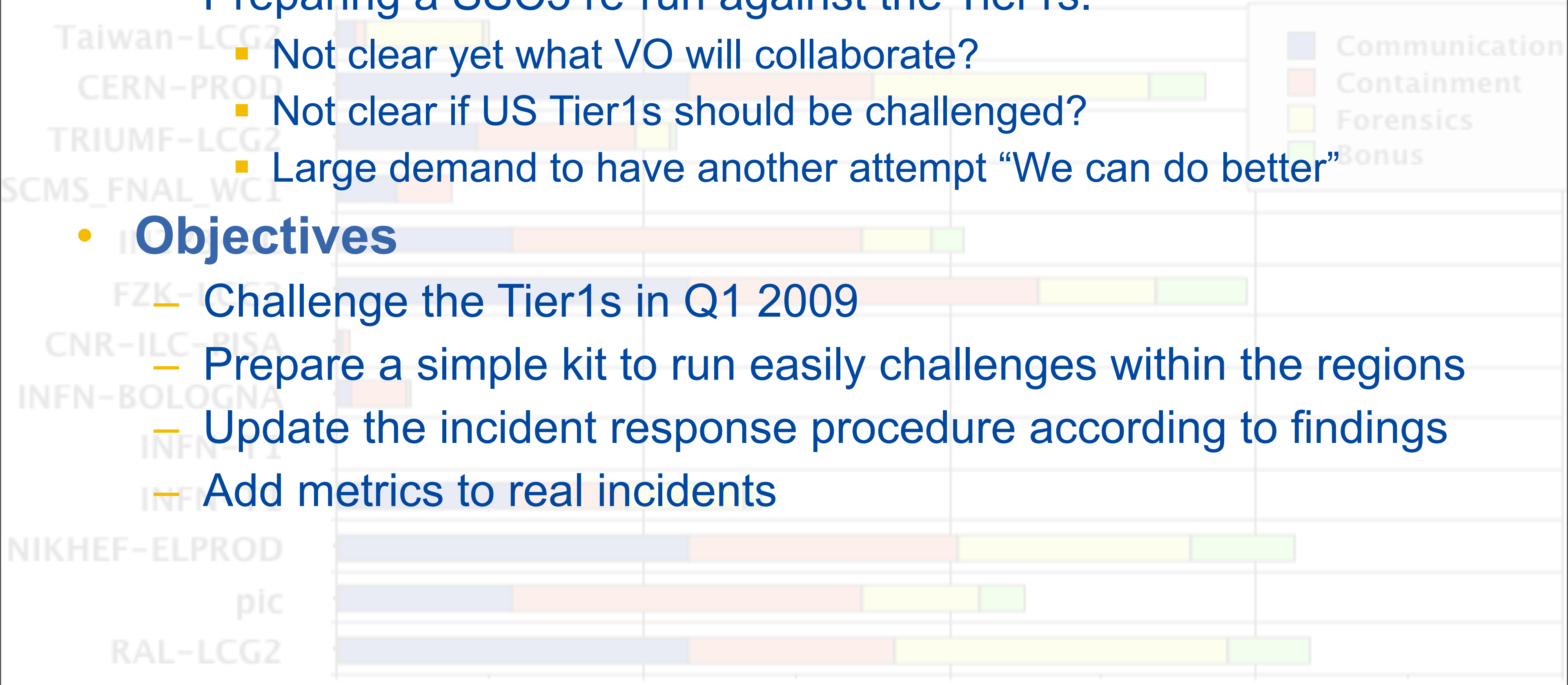
- **Activities now fully coordinated by the ROCs**
  - SWE: Incident Response
  - NE: Security Service Challenges
  - CE: Monitoring and logging
  - UKI: Training and dissemination

- **Cooperation with the NRENs** (now for real)
  - Identified as a priority by the ROCs
  - Discussions during upcoming FIRST/TF-CSIRT and TNC meetings
  - Objective: initial collaboration plan early 2009

- **Improving information sharing with peer grids**
  - Lots of progress already achieved
  - Currently collaborating with OSG, TeraGrid, NDGF & some NGIs

Security Service Challenge

- Activity is now coordinated by NE
- Current work
  - Improving/simplifying the current testing framework
  - Preparing a SSC3 re-run against the Tier1s.
    - Not clear yet what VO will collaborate?
    - Not clear if US Tier1s should be challenged?
    - Large demand to have another attempt “We can do better”
- Objectives
  - Challenge the Tier1s in Q1 2009
  - Prepare a simple kit to run easily challenges within the regions
  - Update the incident response procedure according to findings
  - Add metrics to real incidents



Training & dissemination

- **UK/I is coordinating this activity**

- **Successful training event at EGEE08**
  - Joint event with the MWSG
  - Good feedback received

- **Current status**
  - Lots of material, presentations, sources, etc.
  - Lacks middleware-specific information

- **Work in progress**
  - New website, more structured information (APROC)
  - Discussion with the MWSG to prepare simple procedures:
    - Ex: how to suspend a user on service XXX?

Security incidents

- **6 security incidents in “the grid” in 2008 so far**
- **Several attacks affecting multiple grids**
- **Recurring issues**
  - Leaks
  - Origin of incident not always clear: lack of logging, lack of security expertise
- **Major progress**
  - Improved communications with peer grids
  - Ad-hoc teams during large incidents
  - Incident response procedure more understood and followed
- **In work**
  - Updated incident response procedure (with timelines, metrics)
  - Improve information flow
    - Currently using a broadcast model: 1000+ recipients?

Logging and traceability

- **Essential to understand the cause of incidents**
  - Contain, resolve the incident and prevent re-occurrence
  - Unblock users/sites/VOs
- **“Grid Security Traceability and Logging Policy”**
- **Middleware logging is still a major concern**
  - Middleware not always using syslog
  - Information not always machine readable
- **Site logging remains also a major concern**
  - Not clear what to log
  - SSC should help sites understand their needs
  - Storing the logs is usually not a space problem
  - Processing the data however may take longer than expected
    - Filtering needed?
  - Most incidents usually require 2 -> 6-month-old information

Logging and Traceability

• Draft "Operational Notice": GDB view?

The objective of this operational notice is to specify conditions under which logging information must be retained for longer periods.

The EGEE project has adopted the Grid Security Traceability and Logging Policy policy (https://edms.cern.ch/document/428037/) proposed by the JSPG.

The policy "defines the minimum requirements for traceability of actions on Grid Resources and Services as well as the production and retention of security related logging in the Grid."

In particular, the document specifies that "The level of the logging MUST be configured by all service providers, including but not limited to the Sites, to produce the required information which MUST be retained for a minimum of 90 days. Grid Security Operations MAY define longer periods of retention for specific services and/or operational requirements. The logs MUST be collected centrally at the service provider level."

In addition to retain logging information for a minimum of 90 day as defined in the policy, the following logging information MUST be retained by the sites for a minimum of 180 days:

Node type 1: list of files
Node type 2: list of files

In addition, the policy specifies that the logs "MUST be collected centrally at the service provider level". Sites are strongly encouraged to implement this requirement via a central syslog service (ex: syslog, syslog-ng, rsyslog), which would enable easier filtering, archival, and processing of the logged information.

Example log files

- (Credit to Carlos Fuentes and Daniel Kouril)
- CE
  - Syslog
  - /var/log/edg-mkgridmap.log
  - /var/log/gridftp-session.log
  - /usr/share/tomcat5/logs/glite-ce-cream.log (CREAM CE)
- WMS
  - Syslog
  - ${GLITE_LOCATION_LOG}/httpd-wmproxy-access.log
  - ${GLITE_LOCATION_LOG}/wmproxy.log
  - ${GLITE_LOCATION_LOG}/lcmaps.log
  - ${GLITE_LOCATION_LOG}/logmonitor_events.log
- MyProxy
  - Syslog
- VOMS
  - /var/log/glite/voms.<VONAME>

  etc.