

# Round-table

*Romain Wartel*

*Operational Security Coordination Team*

*OSCT-2 , CERN*

*26<sup>th</sup> January 2007*



*Different tasks for OSCT have been identified.*

*How do the ROCs propose we achieve them?*

*How can we collaborate and share the load?*

*While this list is by no mean exhaustive or authoritative, the proposed tasks so far cover:*

- *OSCT communications with other groups and the sites*
- *Incident Response improvement*
- *Security tools (monitoring, detection, prevention)*

*During this session, all ROCs are welcome to comment on proposed tasks and their priority, and according to their preferences and availability, offer some contribution on one or more area.*

*OSCT needs to deal with sensitive information, but must also be able to communicate with all the sites and other external projects.*

- What is the best way to handle the information flow for unpatched software or operational vulnerabilities? (GSVG -> OSCT -> all sites)*
- How can we resolve or mitigate SPAM problems on the incident reporting channels, while enabling external communities to contact our CSIRTs?*

*Do we need a both a CSIRT and a CONTACTS list?*

*Communication with peer Grids (ex: OSG)?*

- Management of LCG Security Website, OSCT website, Security RSS feed?*
- Training event?*

*(dedicated session)*

### ***1. Existing tools: pakiti, lcg-fw, Grid-wide firewall:***

- ***To we want to advertise them?***
- ***Can we (OSCT) maintain them?***

### ***2. New tools:***

- ***Contributions to build some SAM security tests***
- ***Can/should we re-use other farm/grid monitoring tools?***
- ***Are there other monitoring tools that should be advertised?***

### ***3. Usage by the sites***

- ***Is it possible to centrally publish the output of these tools? If so, how can we implement access control?***
- ***How can we push the tools to the sites?***

***(dedicated session)***

- *Incident response scenarii, Incident response procedure for sites/Incident reporting form?*
- *Security Service Challenge*
- *Incident tracking tool?*