Security Service Challenges in WLCG: SSC3 2009 Results

P. Anderssen[2], S. Gabriel[1], A. Sharma[4], C. Triantafyllidis[3], R. Wartel[2], U. Epting[5], J. Chien[6], M. Mingchao[7], M. Altunay[4], M. Prochazka[8], D. Kouřil[8], R. Brunetti[10], V. Martín-Rubio Pascua[9], C. Fuentes Bermejo[9], A. Sandgren[11], D. Fouossong[12]

[1]Nikhef, [2]CERN, [3]AUTH, [4]OSG (NCSA), [5]KIT-SSC, [6]ASGC, [7]RAL, [8]CESNET, [9]RedIRIS, [10]INFN, [11]HPC2N, [12]CNRS

Enabling Grids for E-sciencE

Mandate/Objective

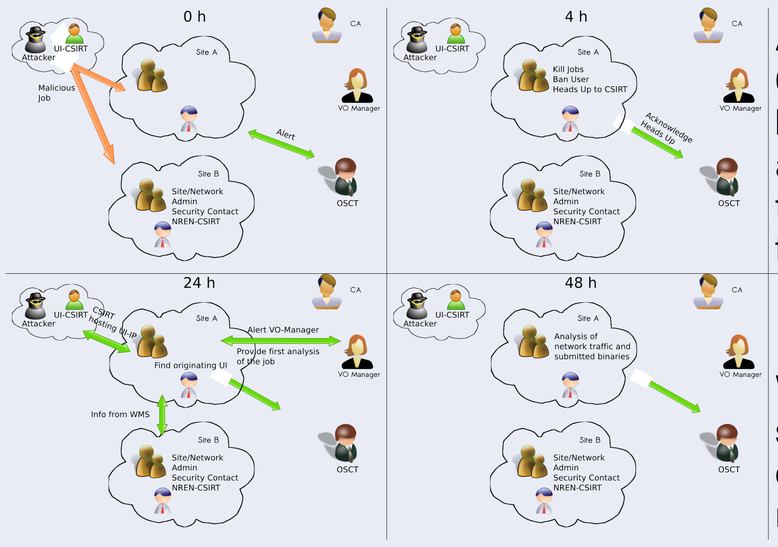
The Security Service Challenges (SSC) are executed under the authority of the EGEE/LCG Operational Security Coordination Team **OSCT** [1] and OSG Security Team. The goal of the LCG/EGEE/OSG Security Service Challenge, is to investigate whether sufficient information is available to be able conduct an audit trace as part of an incident response, and to ensure that appropriate communications channels are available. More specifically, the SSC will address the following security aspects of the Grid:

1. Compliance with, and understanding of, the Audit Requirements for LCG;
2. Compliance with, and understanding of, the LCG/EGEE/OSG Incident Handling and Response Guide;
3. The overall execution of the incident handling procedures.

The SSC3 was designed to mimic a Grid security incident, where a malicious job is run by a user with a legitimate Grid credential. The challenge is intended to test three areas in a security incident handling procedure, namely communication, containment and forensic. The SSC3 in OSG needed some modifications to test environment since different middle-wares are used. The run in OSG was conducted by A. Sharma.

SSC3 - Role-play

The third Security Service Challenge 3 (SSC3)[1, 2] tested the operational diligence of the LCG/EGEE Grid Sites and has been executed at Tier1 sites in the WLCG.



After receiving the alert at 0h the sites are supposed to kill/stop the job, ban the user at their site, notify OSCT and the VO-manager within the first 4h

Within the first 24 h the sites should be able to find the originating UI and contact the resp. CSIRT.

Results: SSC3 Runs 2008/2009 in LCG and SSC3 2009 run in OSG

- **Communication**: All sites improved in this section. I.e. the response times were considerably reduced. The content and the completeness of addressed entities improved a lot. The format of the mails varied a lot, mail templates that can be used in incident reporting/communication are now provided on the OSCT web page (http://cern.ch/osct).
- **Containment**: Compared to the 2008 run this part of the exercise was done by most sites much quicker, in one case from 70 hours to two hours. Many sites were able to save the files associated with the malicious test job.
- **Forensics**: All sites, besides one, improved on the forensics part of the SSC. All sites found the originating UI. Many sites reported that they checked for root kits and that they will -**after finishing the investigation and/or taking a disk image**- reinstall the affected host. Dedicated network analysis was done by approx. 50% of the challenged sites. All sites, besides one, analysed the binary and found the relevant parts.

Figure: Results of the SSC3 runs in 2008 and 2009. Colour coding: Communication (blue), Containment (yellow), Forensics(red), Bonus (green). In grey: difference to Target. For details on the scoring schema see SSC-Wiki.

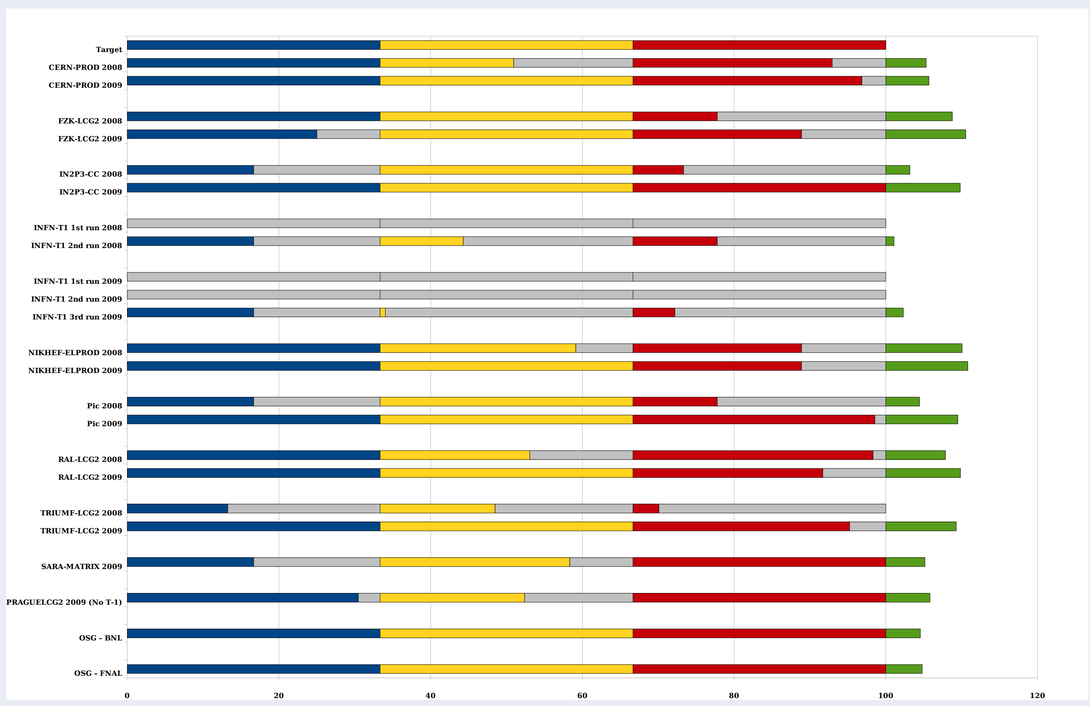


Figure: 1 EGEE-and OSG-T1 Sites

Status of the regional SSC3 Runs

ROC	DECH		UKI		NE				AsiaPacific	FRANCE	RUSSIA
Countries	Germany	Switzerland	United Kingdom	Ireland	The Netherlands	Belgium	Scandinavia	Baltic	11 countries[a]	France[b]	.. see Goc-db..
Number of Sites	23		21		14[c]	5	28[d]		29	15	?
Status SSC3-Run[e]	Completed 17		Completed 19		Completed 19		In preparation		Completed 13	Running 7	No Response

ROC	CE	SEE	SWE		ITALY
Countries	8 countries[f]	8 countries[g]	Spain	Portugal	Italy
Number of Sites	25	12	25		44
Status SSC3-Run	Running 22	Completed 10	Running 9		Completed 25, Running 2

The regional SSC3 runs were conducted by the regional Security-Officers in the respective region, see authors list.

[a]Taiwan, South Korea, China, Japan, Australia, HongKong, India, Pakistan, Malaysia, Thailand and Vietnam.
[b]One Site in Senegal, not yet in production
[c]10 Sites centrally managed.
[d]ARC and gLITE middleware in use, Sweden, Norway, Finland, Denmark, Latvia, Lituania, Estonia, Slovenia, and 2 swiss ARC sites.
[e]Status at Nr. of sites in that region, rest not tested yet.
[f]Austria, Belarus, Czech Republic, Croatia, Hungary, Poland, Slovenia, Slovakia
[g]Bulgaria, Cyprus, FYROM, Greece, Israel, Romania, Serbia, Turkey