Security Service Challenges
in the context of EGEE

ISSeG

Ursula Epting,
Bruno Hoeft, Marc Hemberger

Forschungszentrum Karlsruhe GmbH
Institute for Scientific Computing
PO Box 3640
D-76021 Karlsruhe

http://www.gridka.de

What is a Security Service Challenge (SSC)?

How do SSCs look like?

Practical examples: SSC 1 / SSC 2

Results and problems in the region GermanySwitzerland

Why doing SSCs? - Conclusion

What is a Security Service Challenge? (1)

„The goal of the LCG/EGEE Security Service Challenge is to investigate whether sufficient information is available to be able to conduct an audit trace as part of an incident response, and to ensure that appropriate communication channels are available.“

https://twiki.cern.ch/twiki/bin/view/LCG/LCGSecurityChallenge

It is like a fire service drill!

What is a Security Service Challenge? (2)

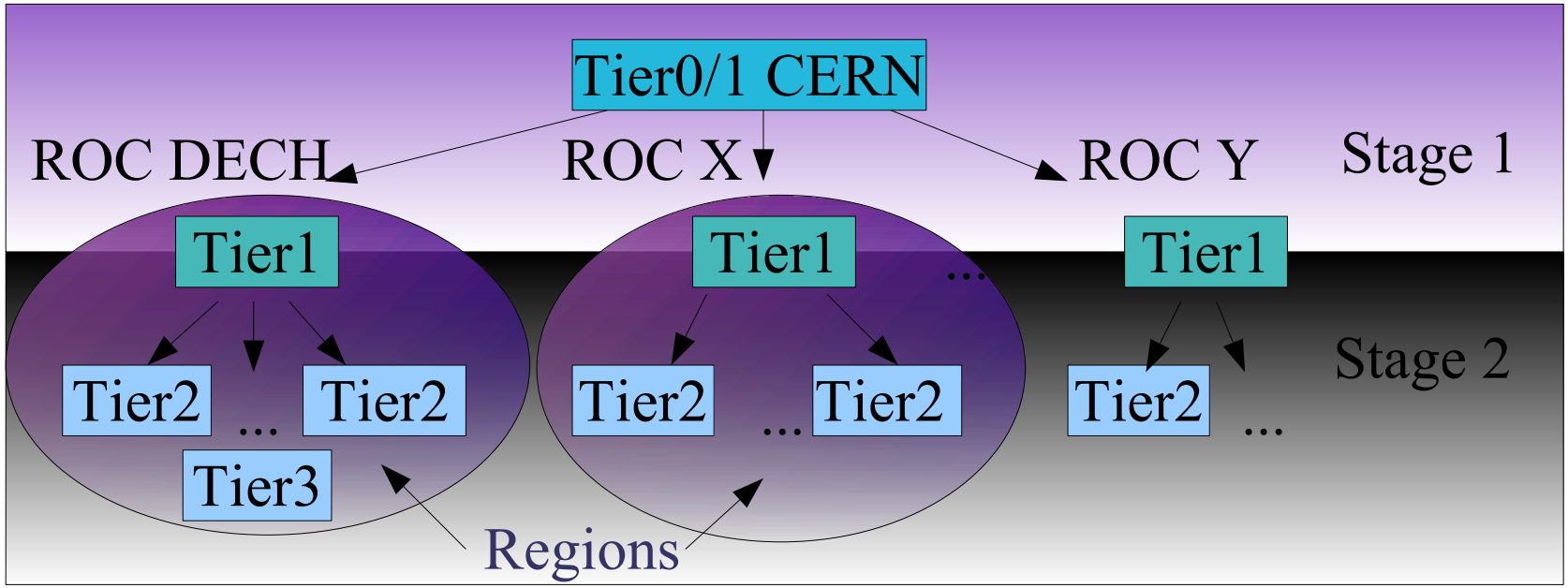
- Exercise if communication between sites is functioning, which is fundamental in a real security incident
- Exercise for admins to trace users/operations and to know which logfiles contain the needed information
- Not intrusive, only 'legal' operations are executed (jobsubmission, file transfer, ...)
- No penetration tests, no execution of exploits etc.
- The kind of challenge is stipulated from Operational Security Coordination Team (OSCT) <= site security officers

How do SSCs look like? (1)

- SSC level 1, challenges the Workload Management System (WMS) on the Grid: Resource Broker (RB) and Compute Element (CE) (2005)
- SSC level 2, challenges the Storage Elements on the Grid (2007)
- SSC level 3, challenges the Operational Responsiveness of the LCG/EGEE Grid Sites (under preparation)

https://twiki.cern.ch/twiki/bin/view/LCG/LCGSecurityChallenge

How do SSCs look like? (2)
Organisation and execution of SSCs



- Stage 1: CERN challenges Tier1 centres in different countries
- Stage 2: executed by the Regional Operation Centre (ROC) within its region, e.g. Tier1 GridKa challenges sites in DECH – GermanySwitzerland

Example: SSC 1

Dear LCG/EGEE ROC Site Security Officer,
This e-mail constitutes a security service challenge alert.

--- Known_Particulars_of_Affected_Site_and_Job --------
Date - 2005_06_01
- and time period of challenge, between: 08:26 -and- 08:37 UTC
LCG/EGEE siteName: FZK-LCG2
Regional Operation Center (ROC): GermanySwitzerland
IP-address of the target computer: c01-013-131.gridka.de
UNIX-UID of challenging job on target: 17002

--- Evidence_sought ---------------------------------
1). The DN of grid-credentials/certificate used by the job submitter?
2). The IP-address of the submitting network device (UI)?
3). The name of the executeable which ran on the target computer?
4). The date and the precise time when the executeable ran?

Details and solutions at https://twiki.cern.ch/twiki/bin/view/LCG/SSC1

Results: SSC 1 (only DECH)

SSC 1	Day 0	Day 1		Day 2	Day 3		Day 4		Day 5	Day 6	Comment
Site	Job submitted	1. Alert			2. Alert		Escalation			Escalation	
A	X	X			X		X	in progress			No site admin nor security officer
B	X	X			X		X		in progress		not solved
C	X	X			X		X		in progress		not solved
D	X	X			X		X			X	Alert email didn't reach site security officer
E	X	X			X	in progress ½ solved					partly solved
F	X	X	in progress ½ solved								Response from RB owner missing, partly solved
G	X	X	in progress	½ solved					solved		all information found
H	X	X			X	in progress solved					all information found
I	X	X	in progress	solved							all information found
J	X	X	in progress	solved							all information found

Example: SSC 2

A sequence of storage operations has been executed on your site as part of a Security Service Challenge (SSC). The particulars of the operations are listed below:

Distinguished Name (DN) of Grid credentials used by the submitter:
/C=CH/O=CERN/OU=GRID/CN=Paul Newman
Date:2006-10-10
Approximate time interval: between: 07:20 -and- 07:40 (UTC)
Affected storage element: lcg-gridka-se.fzk.de

Please investigate and respond by providing the following information:
1). Which sequence of storage operations were executed by the challenger in the specified time interval (UTC)?
2). What was the IP-address of the User Interface (UI) which was used for the job submission?

Details and solutions at https://twiki.cern.ch/twiki/bin/view/LCG/SSC2

Results: SSC 2 (only DECH)

SSC 2	Day 0	Day 1		Day 2		Day 3	Day 4	Day 5	Comment
Site	job submitted	1. Alert		2. Alert					
A	X	--							no support of dteam vo => challenge failed; scheduled maintenance
B	X	X		X	in progress			not solved	not solved due to scheduled maintenance
C	X	X		X	in progress			not solved	No log information available because of a software update on Day 0
D	X	X		X	in progress			partly solved	Security officer was not registered by GGUS ticket system, ui information missing
E	X	X	in progress, partly solved					partly solved	ui information missing
F	X	X		X	in progress			solved	all information found
G	X	X	in progress		solved				all information found
H	X	X	in progress, partly solved		solved				all information found
I	X	X	in progress		solved				all information found
J	X	X	in progress		solved				all information found
K	X	X	in progress, solved						all information found
L	X	X	in progress, solved						all information found
M	Test site		solved in advance						dCache log level adjusted, all information found

Results: SSC 2 (worldwide)

Google map showing 65 participating Grid sites with their respective scores

Why doing SSCs? - Conclusion

- SSCs are necessary for site security officers as training how to react in an incident case
  - this includes internal coordination to get the needed results as well as proper use of the reporting channels
- SSCs are necessary for site admins to get familiar with the logfiles, to learn how to trace users/jobs on their site, and to learn how to react
  - the majority of admins appreciated the tests!
- The knowledge, capability, and willingness to take the responsibility for the site security differs from site to site -
  but keep the Grid running requires close collaboration!

Thanks for your attention!

Questions?

Coffee?? 

Links

- https://twiki.cern.ch/twiki/bin/view/LCG/LCGSecurityChallenge

Google maps for SSC 1 and SSC 2:

- http://grid-deployment.web.cern.ch/grid-deployment/ssc/SSC1.html
- http://grid-deployment.web.cern.ch/grid-deployment/ssc/SSC_2/SSC_2_google.html

Thanks for nice graphics for the fire service drill to:

- www.ff-altenbochum.de
- www.vskrems-lerchenfeld.ac.at

Brandnew: SSC 3 !!!

A persistent Grid Job has been submitted to one of your Sites as part of a Security Service Challenge (SSC). The particulars of the Job are listed below:

The Grid credentials used for the submission were:
/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=pna/CN=310579/CN=Paul Newman
Date: 2007-09-13
Approximate time of submission, between: 06:15 -and- 06:45 (UTC)

Please stop the Job and suspend the Grid access authorization of the incriminated user.
Also, please use the ticketing system to respond by providing the following:
1). The IP-address of the User Interface (UI) which was used for the submission of the Job;
2). A list of the actions that you made;
3). A brief summary of your investigations, complete with an analysis of the programs submitted with the Job.

Having filed the above, you will be alerted through the ticketing system when the access authorization of the user should be restored.
