Karlsruher Institut für Technologie

Security Service Challenges

Ursula Epting

STEINBUCH CENTRE FOR COMPUTING - SCC

Outline

What is a Security Service Challenge (SSC)?

How are they organized?

Practical examples: SSC 1 / 2 / 3 / 4

Tobias Dussa: forensic excursion

Why doing SSCs? - Conclusion

What is a Security Service Challenge? (1)

„The goal of the [...] 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

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 (job submission, file transfer, ...)

No penetration tests, no execution of exploits etc.

The kind of challenge is now designed by EGI-

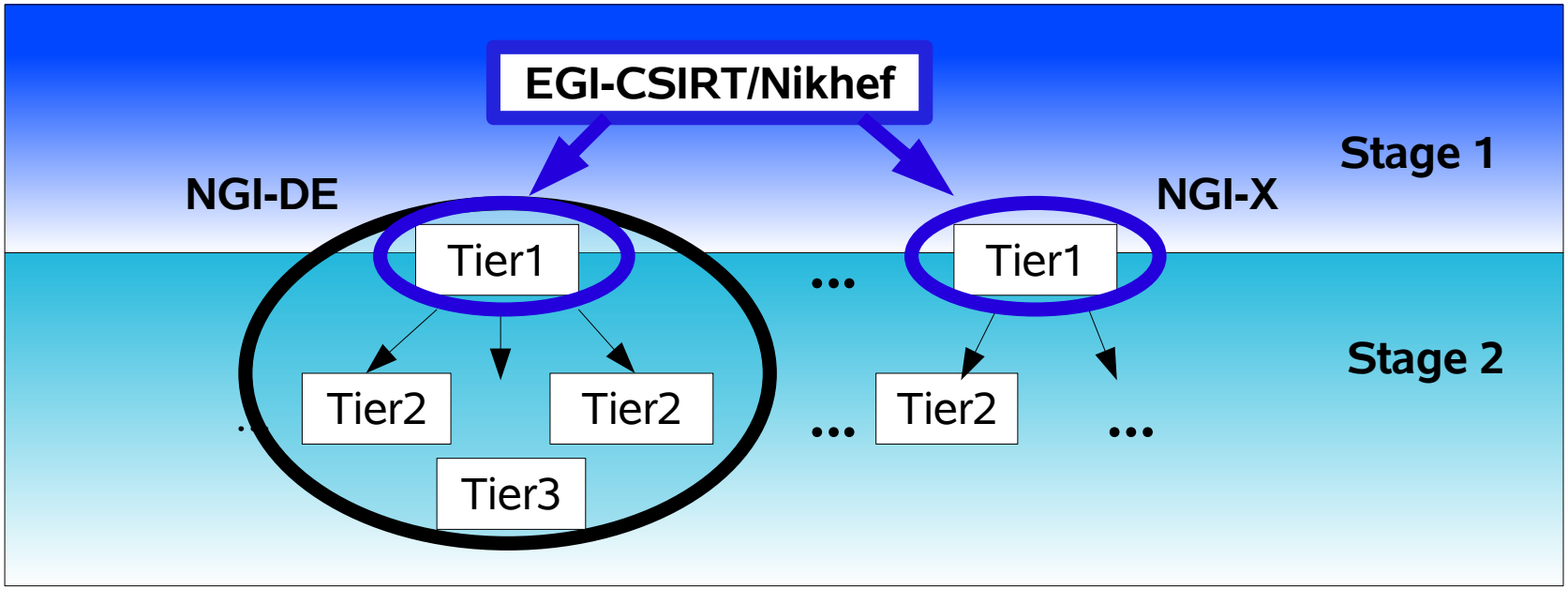
CSIRT (team of site security officers from NGI's).

A Security Service Challenge...

... is like a fire service drill!



Organisation and execution of SSCs
within the EGI-inspire project



- Stage 1: Nikhef challenges Tier1 centres in different countries
- Stage 2: NGI security officer challenges Tier2 centres in his/her region, e.g. Tier1 GridKa@KIT challenges sites in NGI-DE

History - SSC Level 1/2/3

Level 1: A job has been submitted to your site
With date and time period, IP address of the target computer and UNIX UID of challenging job
Find Distinguished Name (DN) of certificate used by the job submitter, IP address UI, name of the executable, date and the precise time when the executable ran?

Level 2: A sequence of storage operations has been executed on your site
With Distinguished Name (DN) of certificate used by the submitter, date, approximate time interval, affected storage element
Find Sequence of storage operations executed by the challenger in the specified time interval, IP address of the User Interface (UI) used for job submission

Level 3: Consider all activities of Distinguished Name (DN) as malicious
Distinguished Name (DN)
Acknowledge/Heads-up report to CSIRT list, Alert to VO Manager,
Verify notification of the responsible CA, Final report to CSIRT list
Find jobs and kill them, suspend the user at the site
Discovery of initiating site (UI) and contact with that sites's CERT, analysis of network traffic, analysis of the submitted binaries

SSC Level 4

Level 4: Consider any network activity of two IPs as malicious

The following slides are kindly provided by Sven Gabriel, NIKHEF/ EGI-CSIRTeam, but they are secret and are not published here, sorry!

Tobias Dussa: forensic excursion

Why doing SSCs? - Conclusion

SSCs are necessary for site security officers

- as training how to react in an incident case
- to improve local incident procedure

SSCs are necessary for site admins

- to get familiar with the logfiles
- to learn how to trace users/jobs on their site
- to learn how to react

Site security differs from site to site -
but keep the Grid running requires close collaboration!

LHC has started

=> Grid will become more and more popular

=> Security incidents will become more probable
We must be prepared!

Karlsruher Institut für Technologie

Thanks for your attention!

Questions?

Coffee??

Links

Security Service Challenges

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
- Thanks for nice graphics to
  www.ff-altenbochum.de
  www.vskrems-lerchenfeld.ac.at

EGI Projekt: http://www.egi.eu/

EGI-CSIRT (public):: https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page

Thanks to Sven Gabriel (Nikhef/EGI-CSIRT), who kindly provided slides 9 to 14 (which are unfortunately not published, sorry!