Security Service Challenges

testing our incident response capabilities

Sven Gabriel (Nikhef), Ursula Epting (KIT-SSC)
EGEE Operational Security Coordination Team
http://cern.ch/osct/

www.eu-egee.org

Outline

- SSC3-9.02 at T-1s
  - Results (for details see poster)
  - Debriefing Sites Feedback
- Regional SSC3 Runs
  - Experiences in ROC-NE (Benelux)
  - SSC3 Run in ROC-DECH (Ursula Epting)

Introduction

- Security Drills are a lot of work.
- We have to find a way to make optimal use of the results.
- Collect experiences of regional runs centrally.
- Regional runs are more ”interesting” than T-1 runs:
  - Regions are more heterogeneous.
  - Consist of many countries, organize meetings more complicated.
  - Communication problems, technical/others ?
  - Centralized Site-Management, and problems related to this.
  - Site Security Teams do vary a lot.
- Feedback needed from regions: What is missing (Tools), What to address (Grid-components), Scoring Schema, ...

Questions to T-1 sites

Is the network and the grid services managed by different people/group? if so did this group/people got involved with the current SSC3?

- At four sites the network is managed by the same people as the middle ware services. At three sites the network is managed by a separate group, which can be asked for help when needed -in this SSC3 it was not necessary).
- *Is a contact to the local NREN known that could assist during a real incident? Was the local NREN involved in the current SSC3 run?*
- At all sites a NREN-CERT Contact is known, at two sites the NREN-CERT got involved in the SSC3.

Questions to T-1 sites

Which fabric (site) management tool is in use (yaim, cfengine, quattor, ??)

- All sites use a dedicated fabric management (quattor:3, cfengine: 2, puppet: 2) in combination with yaim.
- *How is user-banning done, site centrall with these tools?, ”by hand?”*
- Two sites did security operations like user banning centrally using their fabric management tool, other sites locally on the affected hosts. By part this was due to incomplete deployment of the fabric management and might change in the future.

Questions to T-1 sites

Additional Tools:

- *How (if) is the WN checked for root compromise?*
- Three sites have checked for root kits, two of them run checks frequently. Four sites have not checked for root kit.
- *Is there any intrusion detection system running at the site, if yes which?*
- Dedicated intrusion detection systems are currently not deployed at the sites, but four sites are currently planning on this.

Questions to T-1 sites

Your Opinion: *Was the challenge useful?*

- *Almost all sites considered the SSC3 as useful,*
- *Two sites appreciate these tests since it helps them to practice and improve their incident procedures and techniques which otherwise may only be used in case of a real incident.*
- *One site mentioned that the point in time was not optimal.*
- *One site mentioned that it was not clear to them what to investigate (executable, network).*
- *One site mentioned that the SSCs "seems to be focused more on the evaluation of the expertise of the people than on the verification of the procedures'.*

Questions to T-1 sites

Anything you would like to be added/removed?

- One site suggests to run a SSC on the storage systems, targeting the data management services (SE, FTS, LFC).
- One site found the UI-discovery part not realistic since they don't necessarily have the needed log files, i.e. those from the WMS. They suggested to change this to reporting the WMS's CSIRT.
- Three sites mentioned that the alert mail could be improved, in particular it was not clear who send the alarm mail (Remark: Mails were signed).
- The e-mail subject could be more "clear".

Questions to T-1 sites

Do you think you could score better?

- All sites, besides one that did not gave an answer to this, think they will score better in the next run.
- The sites also mentioned, that the procedures at the sites got improved since last run, as well as that the procedures will be revisited after this campaign.

Questions to T-1 sites

- Feedback/Experiences from Security-Officers conducting the SSCs.
- What to improve:
- One feedback-sheet missing, not followed up.
- Automated checks for successfull user banning.

Preparing/Running Regional SSC3

TestOperator (TOp) is attacker and incident coordinator and ...

- Get/Install SSC software from svn repository.
  - Malicous binary (might need some tweaking)
  - Job-Submission framework (scripts). Available for gLite, globus (Aashish).
  - Job-Monitoring webserver.
- Certificate, VO and all the rest.
  - Get a grid certificate (short lived) for the TOp.
  - Negotiate an identity used for TOp with a VO (this VO has to be supported by all sites).
  - Make sure the default communication channels to the sites to be challenged work.
  - Check sufficient queue length/WallClockTime. 72h nice, everything less needs some additional tweaking, but possible. Min. is 12h.

Regional SSC3 Runs -Status

- Status: for details see the poster (43).
- Good coverage, almost all regions started the SSC, some finished.
- NE-Scandinavia-Baltic will be a challenge itself.

SSC3 Set-up in ROC DECH

- Role attacker: Sven
  - Certificate needed.
  - VO (preferably one that wants to play an active role).
  - Job-Submit/Monitoring framework (already available).
  - List of sites, i.e. /ROC/SITE-NAME/requirements.cfg.
  - Submit jobs, check if they “survive” long enough.
- Role Incident Coordinator: Ursula
  - Find suitable VO (CPUWalltime $\geq$ 12h) supported by all sites.
  - settle communication to the sites.
  - Prepare mails to sites/CA/VO, Announce SSC.
  - Send reminders, collect late responses
  - Start the challenge talk/write a lot to sites asking.

SSC3-DECH Timeline

- 15th **June Start of preparation**
  - 15th July Check of validity of csirt addresses, heads up with information about SSC3
  - 17th July Reminder and information about current incident response procedures
- 20th **July Start of execution of challenges**
  - 21th July Reminders sent to not reacting sites
- 29th **July End of challenge**
- 3rd **August Start of evaluation**
  - 11th August End of evaluation, sending evaluation sheets to sites with call for feedback to the sheets and targeted questions.
  - 21th August End of feedback collection
- 22th **August Preliminary report finished** and sent out to site security officers and ROC DECH Management
- 24th **August Holidays :)**

SSC3-DECH Execution/Evaluation

- Execution
  - Start on 20th July, jobs submitted at approx 08:00 localtime.
  - alerts send before 11:00 am, latest 15:30
  - First responses already 20 min. later.
- Evaluation
  - Started on 3rd August
  - Report/request for feedback send out 11th August, 7 sites $<$ 50% provided feedback.

Incident Coordinator Feedback

- Took (much) more time than expected.
- Running the challenge against (almost) all sites in parallel not good (some sites need more attention than others).
- Evaluation very time consuming, clear guidelines what was expected are not available (remark: and can not be given).
- Evaluation done by 2 persons separately, both reports were sent to the sites with the request for feedback.
- Second (re)evaluation round started.
- Results (to be presented by Ursula)
- Next run: Sort out any problems sites may have with motivation to run theses challenges. Avoid as much as possible potential discussions during the challenge

Thanks

Pål Anderssen

Discussion

- How to improve responsiveness of security contacts?
  - Response times in operations policies?
  - What are the experiences in the regions?
  - Have you personaly met with the security contacts?
  - Do the security contacts know you and your role, who is the one to introduce you?
- Additional Communication/Tracking/Ticketing tools needed?
- Centralised Site Management, Chances / Risk?
- Intrusion Detection Systems, some sites plan to deploy IDS soon, how to share experiences?