Enabling Grids for E-sciencE

Security Service Challenge Run 02/03 2009 Preliminary Results

Sven Gabriel, Nikhef
EGEE Operational Security Coordination Team
http://cern.ch/osct/

www.eu-egee.org

e-infrastructure

Information Society and media

CAPACITIES

Thanks

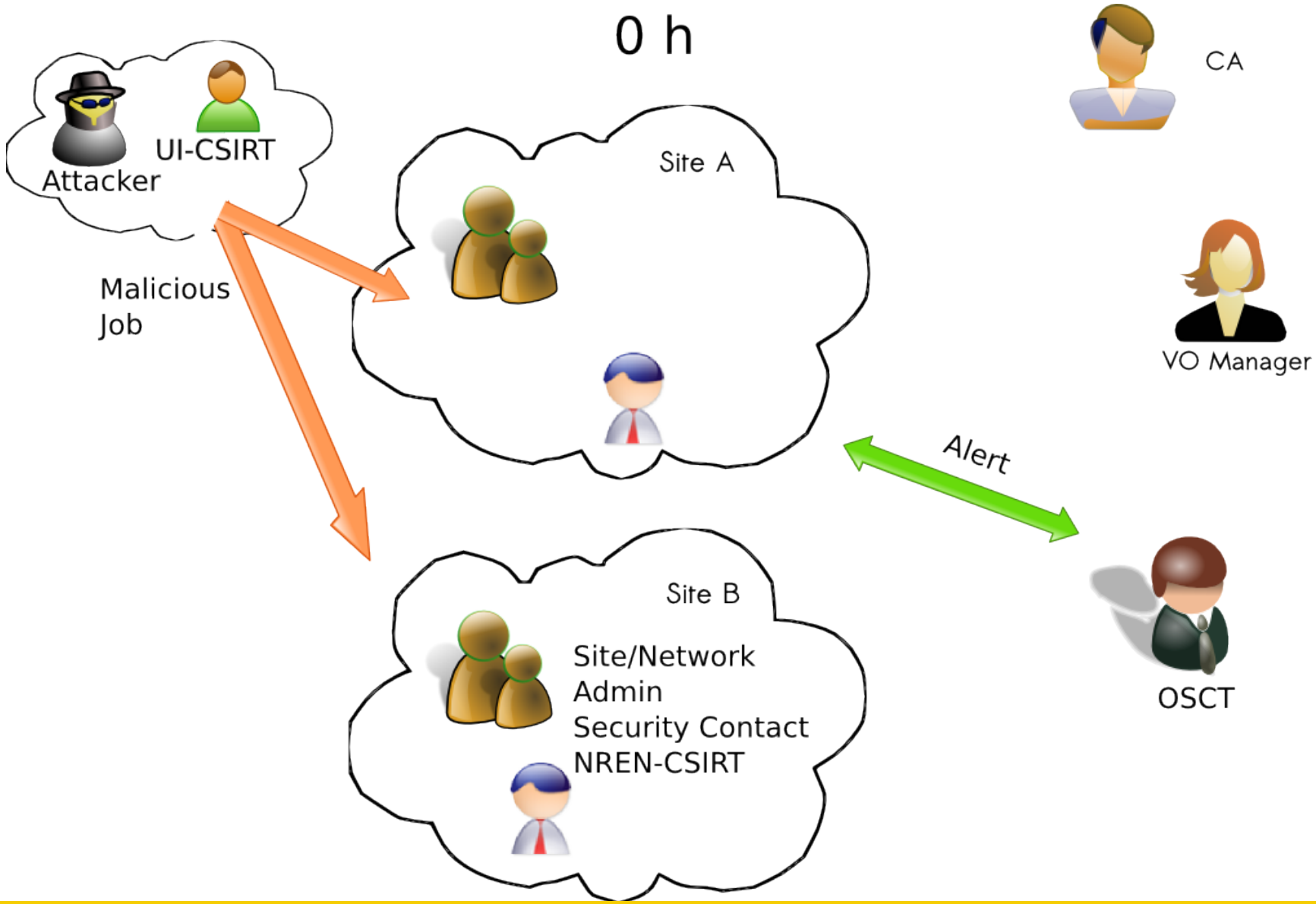
- Pål Anderssen, CERN.
- David Groep, Nikhef.
- All participating sites.

- Atlas VO.

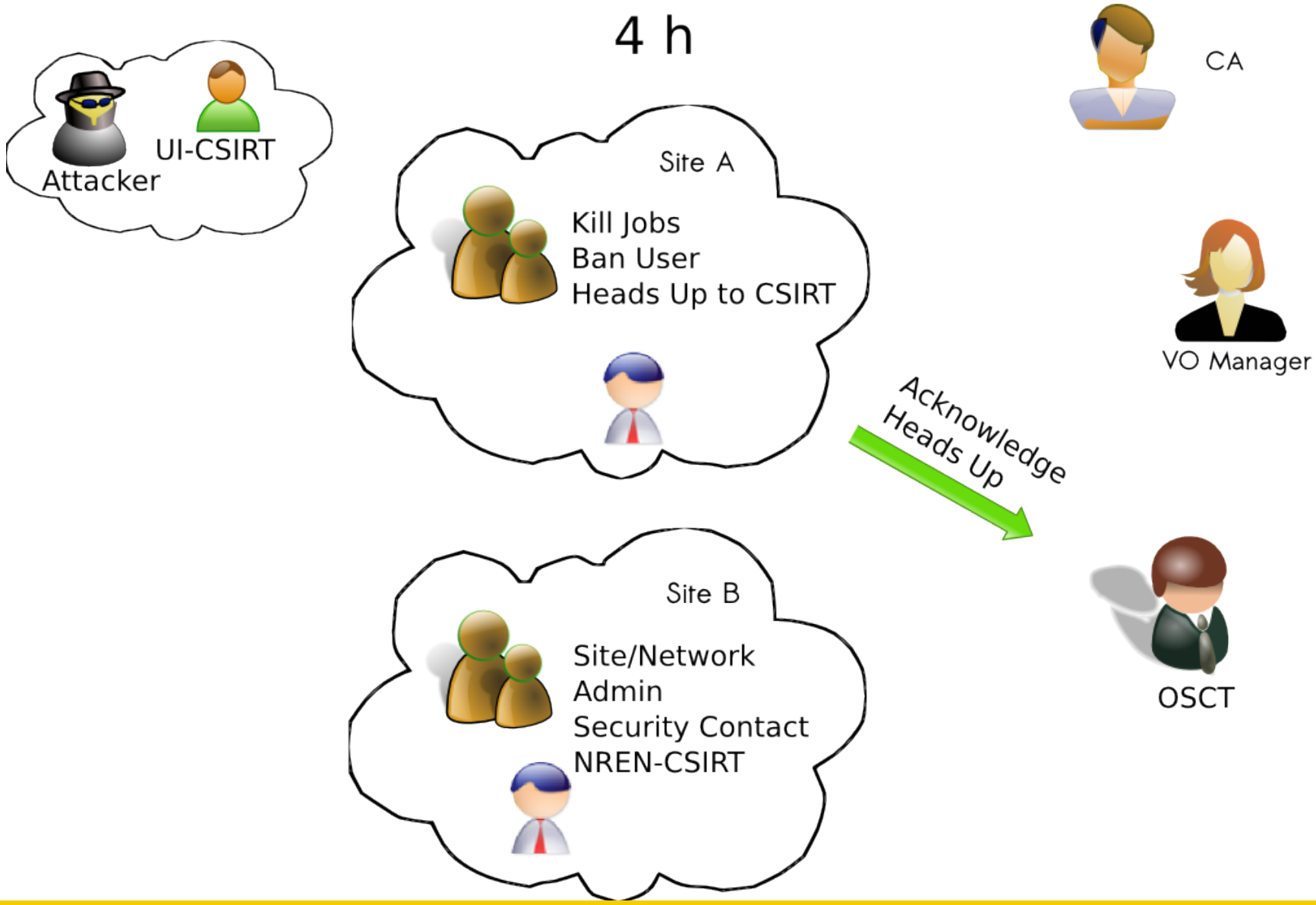
SSC history

- SSC1: Trace a job (WN $\rightarrow$ CE $\rightarrow$ RB $\rightarrow$ UI).
- SSC2: Trace storage operations (file create, move, delete,...).
- SSC3: Realistic simulation of a security incident. “Consider any activity from the following user as malicious. DN: ....”.
- SSC3-9.02: SSC3 rerun. Replaced RB with WMS.

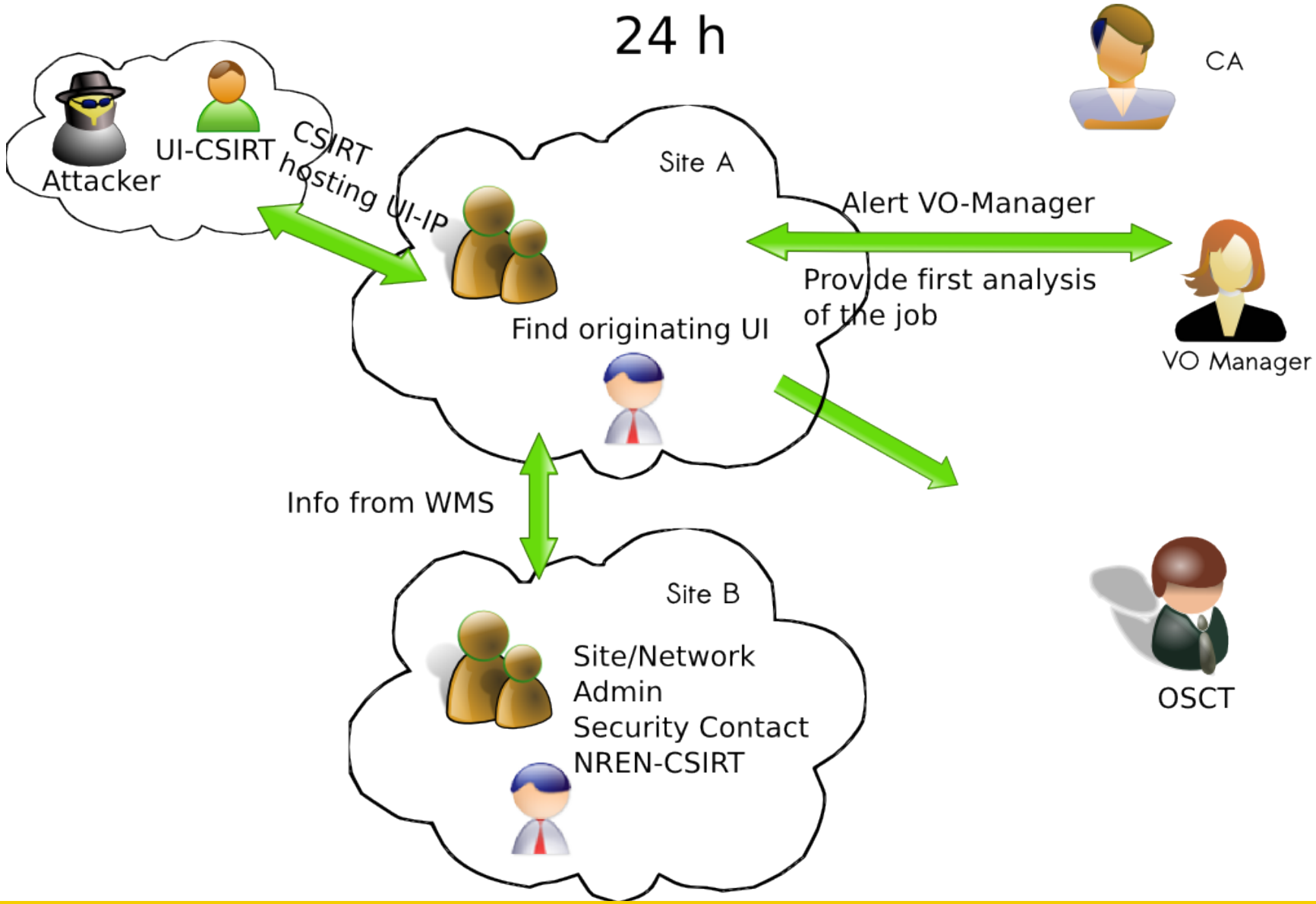
SSC-Roleplay



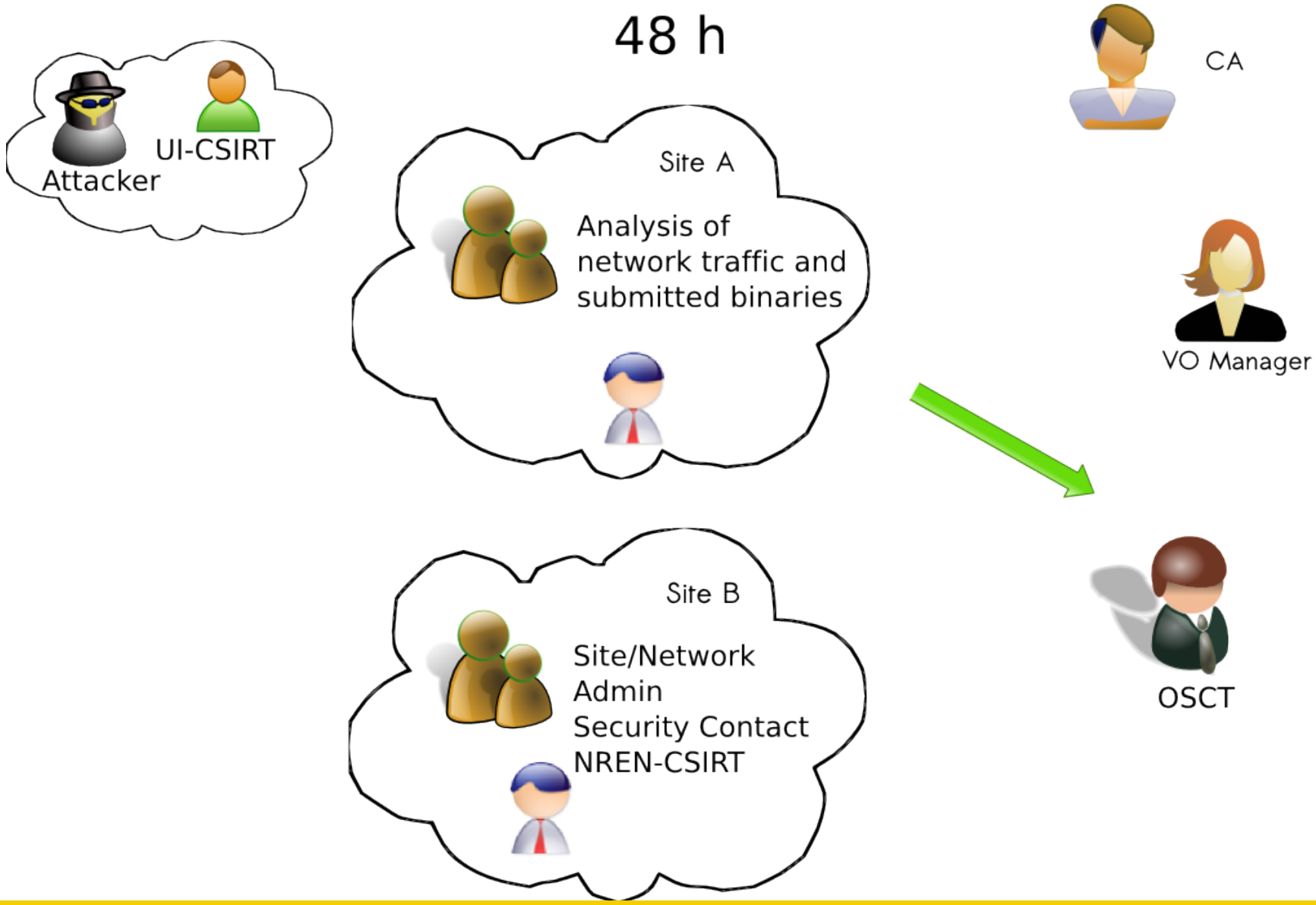
SSC-Roleplay



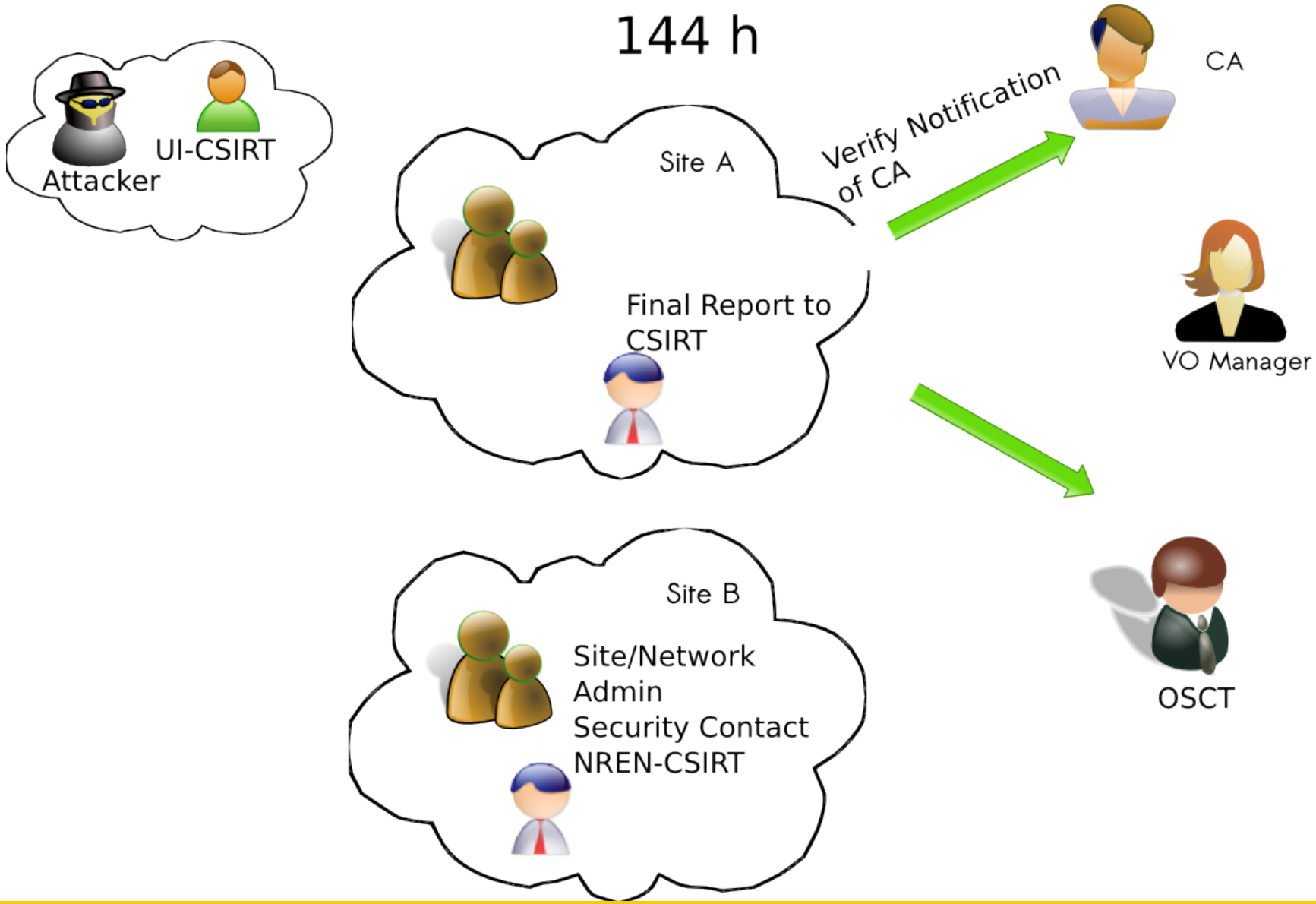
SSC-Roleplay



SSC-Roleplay



SSC-Roleplay



The Task / Job

- The same run as SSC3 besides:
  - Run was announced during OSCT weekly phone meetings.
  - Sites got informed about the evaluation schema with the alert mail.
  - WMS instead of RB.

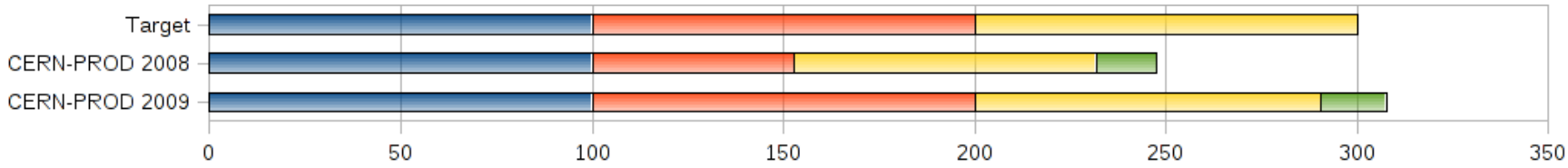
The Task / Evaluation

Evaluation, 3 areas -Time Matters: Bonus Points for fast reactions/pre-reports.

- Communication
  - Acknowledge/Heads-up report sent to the CSIRT list (Target 4h).
  - Alert sent to the affected VO Manager (Target 24 h).
  - Verify the responsible CA has been notified (Target 144 h).
  - Close-out report sent to the CSIRT list (Target 144 h).
- Containment
  - Found the malicious job and killed it (Target 4h).
  - Suspended the user at the site (Target 4h).
- Forensics
  - Discovery of initiating site (UI) and established contact with that site's CERT (Target 24h).
  - Found evidence of malicious network traffic (Target 48h).
  - Some analysis of the submitted binaries was performed (Target 48h).

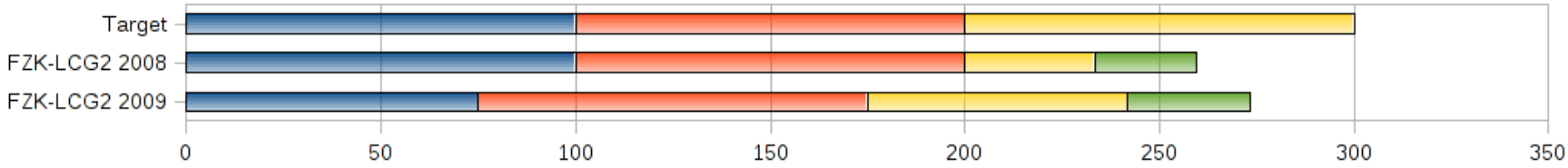
SSC3-9.02 Map

CERN Results



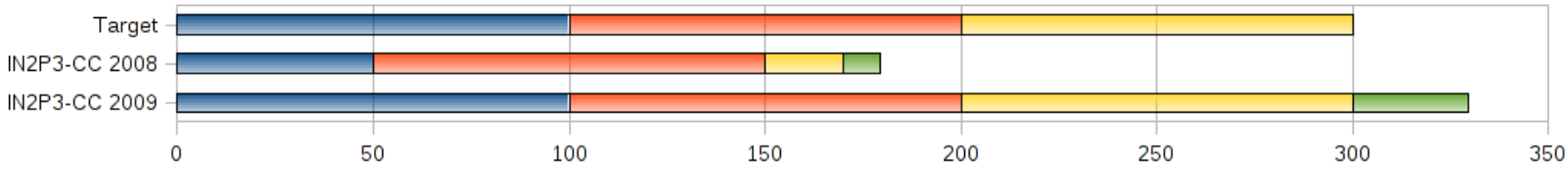
- General remarks
  - Also checked other services (SRM (Castor), LFC, FTS) for the TOp DN
  - Traceback to originating UI (only) in summary -therefore late, not full points for this subtask.
  - Checked for root compromise no evidence found, to be safe WN will be reinstalled.
- Progress since last SSC-run.
  - Killing the job much quicker now: 2h last run: 70h
  - Network traffic from/to WN/Web-server described.

FZK-LCG2 Results



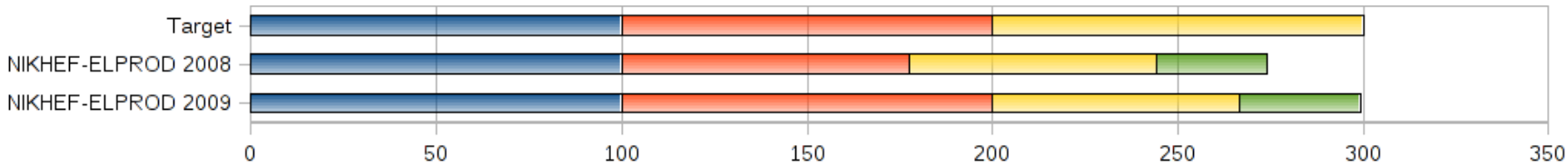
- General remarks:
  - Acknowledge and Heads-up in separate mails
  - Unclear to the site if the user actions are outside the VO-atlas permissible usage of grid resources?, therefore:
  - Communication to CA left with the VO-Managers. A heads up to the users home CA should anyway be send.
  - Contacting the user delegated to VO-Managers, but no details of the job provided.
  - No Network analysis done.
- Progress since last SSC-run:
  - Binary analyzed. Provided an overview of what the binary does/tries to do.

IN2P3-CC Results



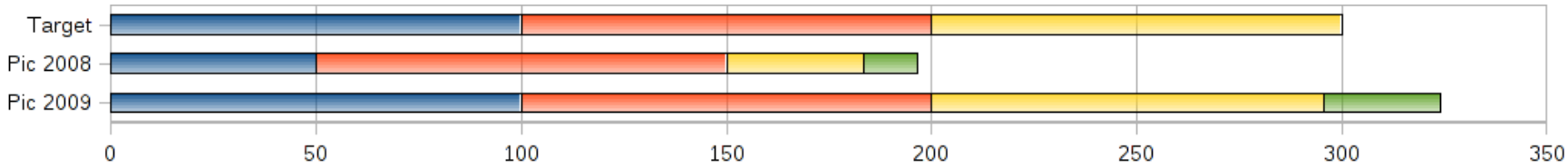
- General Remarks:
  - Timeline provided in the final report.
  - WMS off site, communication worked, Other sites in french ROC informed, all sites acknowledged within 4 h.
  - NREN-CERT (certsvp@renater.fr) and CSIRT of originating UI informed (Dutch ISP).
  - std.out, std.err of the malicious job provided.Checked for root compromise.
- Progress since last SSC-run:
  - Communication complete, in time
  - Forensics communication to web server found, analysis of the binaries done with strings and lsof command.

NIKHEF-ELPROD Results



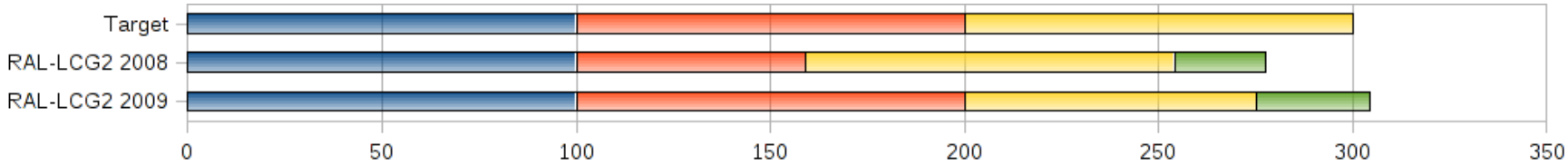
- General remarks:
  - The CA as well as the ROCs security officer already had a role in this simulation and would have been involved in case of a real incident.
  - Local time zone indicated, All reported actions associated with a time stamp.
  - Only site that blocked the originating UI.
- Progress since last SSC-run:
  - Killing the jobs much faster (1.5h 2009, 7.3h 2008)

PIC Results



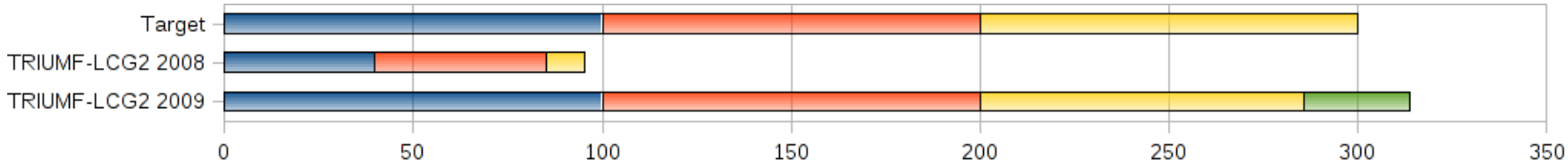
- No clear timestamps in reports, mails from manager on Duty, Gerhard, no phone number, or address in the mails.
- NREN-CERT (RedIris) and CSIRT of originating UI informed (Dutch ISP).
- Progress since last SSC-run:
  - Reporting to VO-Managers done.
  - Reporting to CA done.
  - Originating UI found, CSIRT informed.
  - Network analysis improved.
  - Binary saved for analysis.

RAL-LCG2 Results



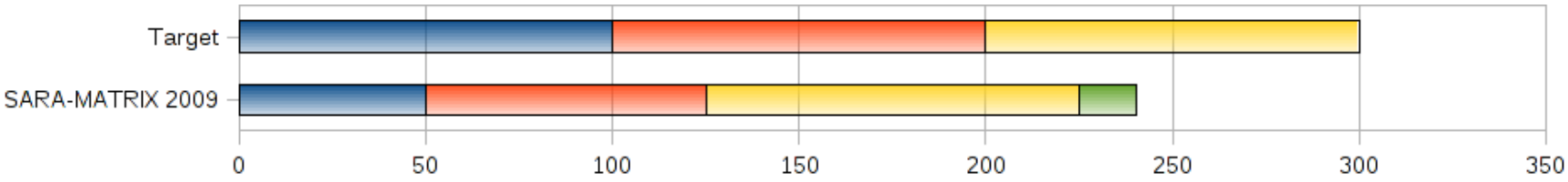
- Jobs efficiently stopped/killed, forked processes found.
- User banning for CEs and WMSs.
- Mail to CA signed (smime.p7s).
- Finding 1: Blocking a user from a MyProxy server not possible.
- Finding 2: problems in local setup, provided solution
- Found detached processes that continued to run after signalling the job to stop.

TRIUMF Result



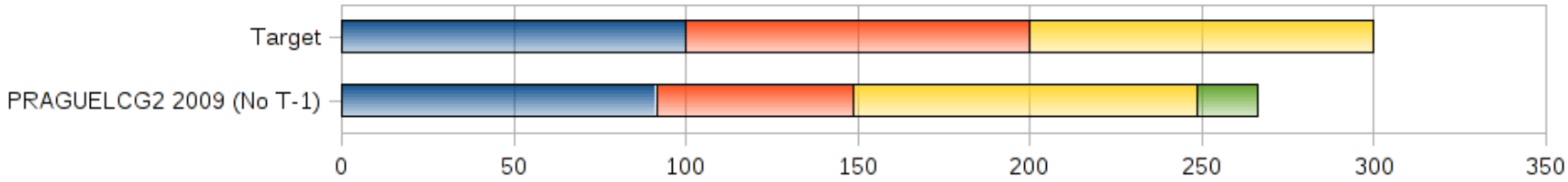
- Remarks:
  - Final report contained the profiler.cfg, std.err, std.out files
  - Requested banning of TOp on the nikhef-WMS
- Progress since last SSC-run
  - Communication more complete, much quicker, only missed the UIs CSIRT
  - Killing the Job much faster.
  - Job tracing done, all involved services found.
  - Network analysis: Mail traffic found.
  - Analysis of the binary much quicker. (156h vs 21.5h now)

SARA-MATRIX Results



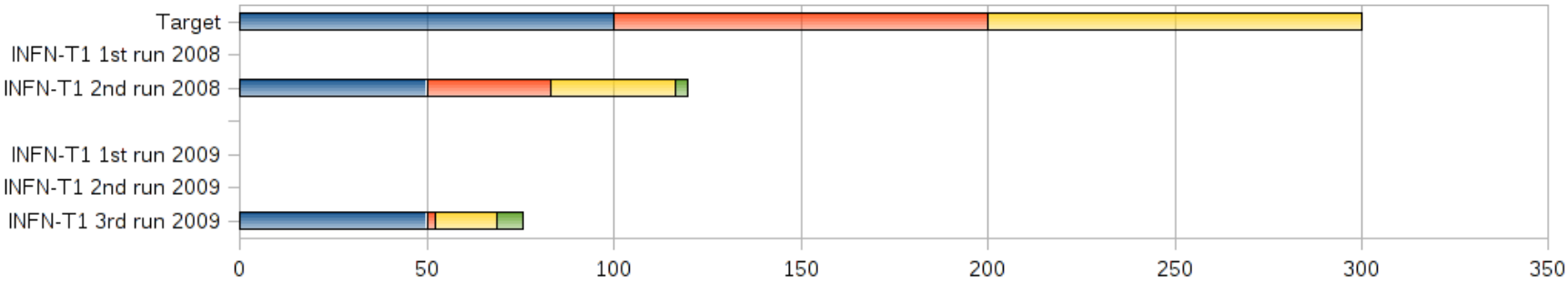
- All mails signed.
- Challenged as part of the federated NL-T1.
- Security-Contact published in goc-db does not work properly, site had to be contacted by another address, meanwhile solved.
- VO Managers got job details, as the url of the web server, that the job is tries cron and at job installation and, that the job ran under suspicious name.
- Final report contained the input sandbox files.
- Jobs killed with the batchsystem, found that job with parent pid 1 can not be killed by the batchsytem.

PRAGUELCG



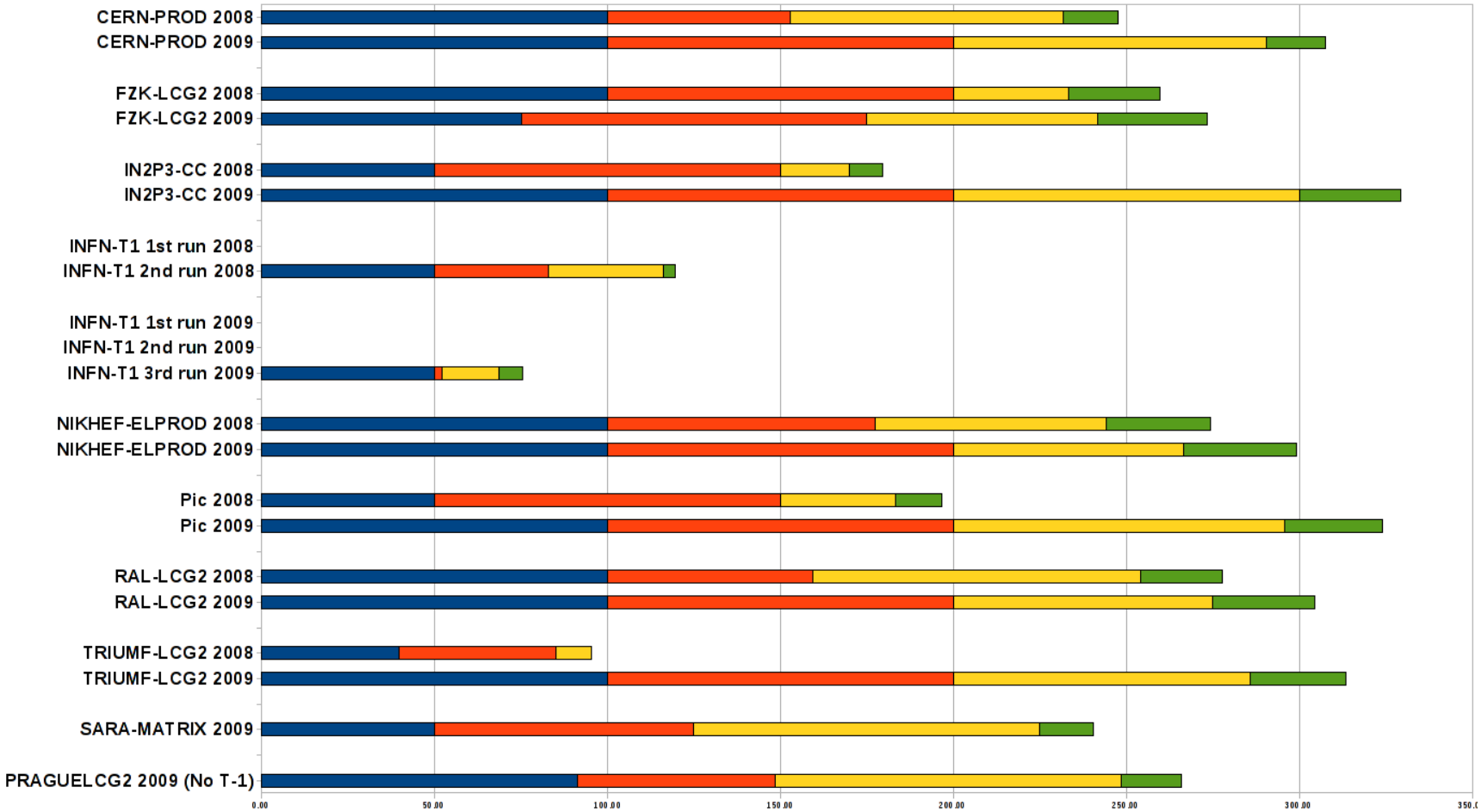
- General remarks:
- PAGUELCG2 is not a T-1, Mails by part signed, checked SE for TOp traces.
- Only! site that provided Network-Traffic-Analysis, done by NREN CESNET.
- Only! site that provided a MD5 sum of the binary.
- Checked for privilege escalation -not found, therefore WN not reinstalled.
- Reporting and Containment took a bit too long, email traffic not detected -so not full points achieved.
- Found cron, at -deleted these, cron/at problematic found, recognized.

INFN-T1 Results



- General remarks:
  - 2008: THIS IS A TEST is misleading.
  - in Total 5 challenges, none passed.
  - Spend a lot of effort in restructuring the Security procedures.
  - 2009: Site did not react, the alert mail was sent 3 times on: *Thu Feb 26 11:24:24 2009*, Mon Mar 2 12:56:01 2009, Tue Mar 3 10:45 2009
  - After asking ROC security contact for help the site did react.
  - Site mentioned that "*all the people involved in the incident response at CNAF were off-line on Monday Mar 2*".
- Progress since last SSC-run: ?

Preliminary Results



Highlights

- Clearly an overall improvement!
- SSC provide input to *Incident Response Procedure* as well to *Training/Dissemination* and vice versa.
  - Network Analysis, Fabric-Management and Security Tools
  - Communication templates needed (now in draft state)
- MD5SUM of binary, input sandbox
- Contact NREN CSIRT about ISP
- Problem with qdel/PPID 1
- Site setup problem, single account at batch system for a group.
- MyProxy Server, ...

Summary and Discussion

- Benefits:
  - Overall SSC3 results clearly improved, both on timescale and quality of the sites actions.
  - Sites can test their procedures, reveal operational problems.
  - Debriefing in progress, wait for feedback from the sites.
- To get an overview the SSC3 is currently run in the regions AsiaPacific Benelux, finished in UK, SEE).
- OSG: SSC3 is about to start, actively porting the software to their framework.
- NDGF: In preparation.
- SSC2 (storage) rerun should be done soon. Simulate storage abuse (currently discussed).
- Another SSC3 (slightly modified, treat IP as malicious) run to improve Communication (site-internal as well as to VO, CA) Before data taking?