Security Drill SSC4 run 2010

Sven Gabriel, Nikhef (EGEE-OSCT/EGI-CSIRT)

- Thanks
  - Atlas VO
  - Graeme, Sander Klous (Nikhef), Andrej Filipcic (ARC), Dutch/UK CA
  - Nikhef SSC-team: Oscar Koeroo, Aram Verstege, Tristan Suerink
- Outline
  - SSC3 recap / Whats new in SSC4
  - SSC4 Setup
  - Evaluation / Sites Results
  - Summary
  - SSC4 Future Runs

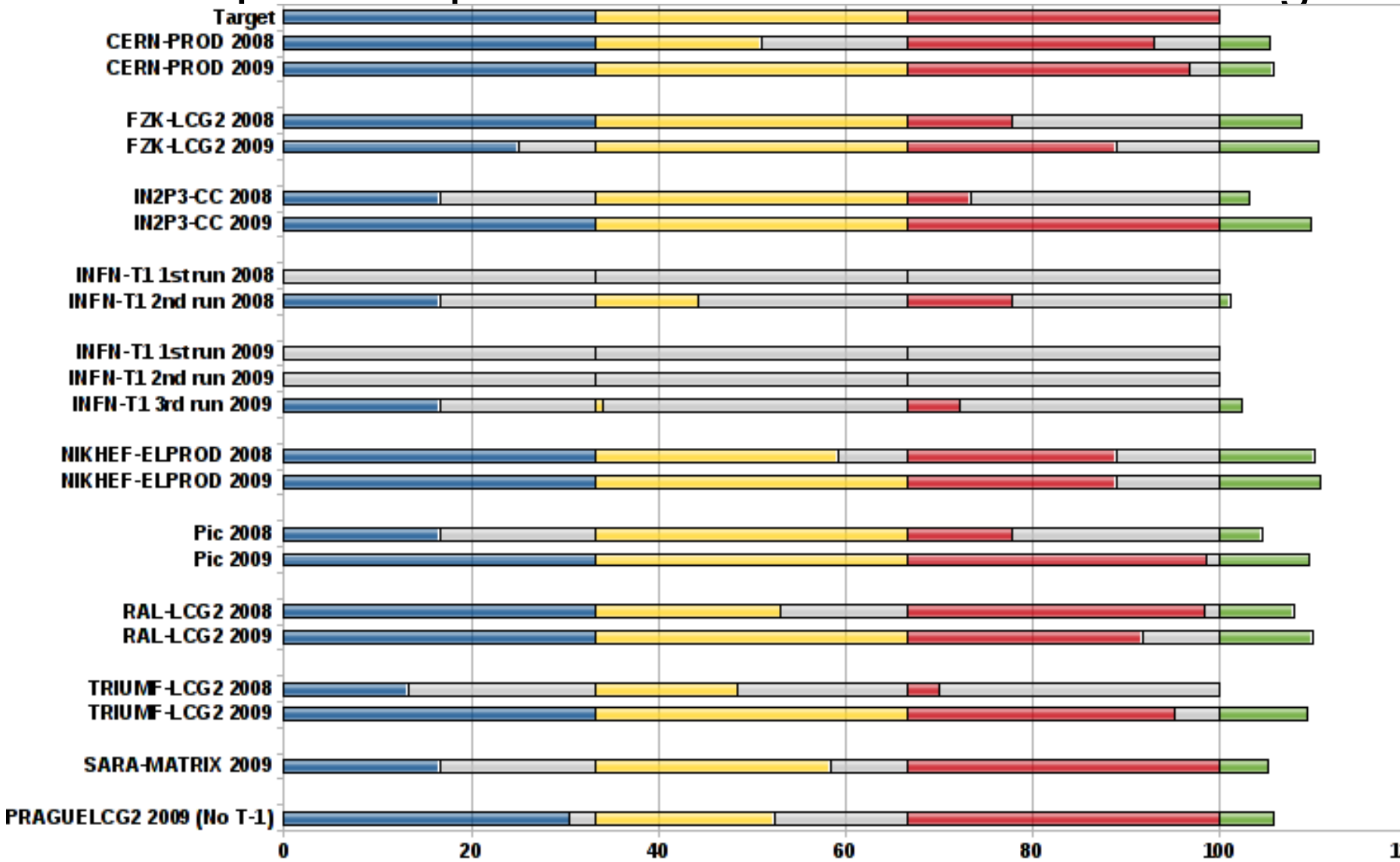
SSC3 Recap: Set-up differences /Results/Debriefing

- SSC-1/2 Basic Incident-Response, Contact-Addresses, Information available (logfiles)
- SSC-3 Alarm: activities related to DN.. / Network traffic between IP1 – IP2
- Involved Components: (myproxy-VOMS), WMS, lcg-CE, WN / Atlas-Job-Submission
- ”Malicious binary” changed
- Evaluation (available to the sites):
  - Communication (What/to who, expected time)
  - Containment (kill jobs, user/certificate Management, save ”malicious software”)
  - Forensics (Network endpoints, protocols, ”malicious software”)

SSC3 Recap: Set-up differences /Results/Debriefing

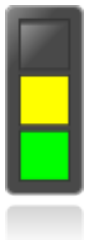
- Almost all sites improved in all evaluated sections
- Communication (Mail): Response times reduced, content and completeness improved ... but, Format to be improved.
- Containment: Find/kill Jobs, User-Management (banning) much quicker, malicious software saved at most sites.
- Forensics: UI found by all sites, network analysis only by some sites, analysis of the binary done by all sites.

SSC3 Recap: Set-up differences /Results/Debriefing

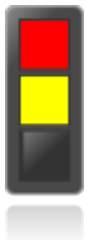


Glossary

OK, Helpful to resolve the incident.



OK, could be improved



Not OK, hard to use for incident response.

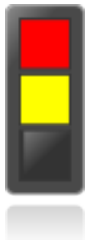
Not sufficient.

PJS Pilot-Job-Submitter, DN under which the pilots run at the sites: graeme andrew stewart (ssc4), for ARC: Andrej Filipcic (SSC4).

PJU Pilot-Job-User, DN under which the job is submitted to the VO-Job-Repository: Sander Klous SSC4)

SSC4 result: ARC Jožef Stefan Institute, Ljubljana, Slovenia

- Communication:
  - Only one mail send. Mainly info from alert mail (connection end points).
  - Only SSC4 Pilot-Job-Submitter DN:Andrej Filipcic (SSC4) found.
  - log file dumps provided extracting relevant information.

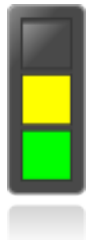


- Containment:
  - Malicious jobs only partially stopped daemon, angel not stopped.
  - No banning, argument: *"We have omitted banning the DN due to the SSC4-related nature."*

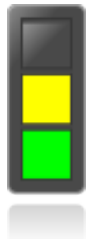
- Forensics:
  - Originating UI not found, information on network traffic/binary only in log file dumps

SSC4 results: CERN

- Communication:
  - Heads-Up to EGI-CSIRT in 30 min. with DN of PJS-Cert.
  - Heads-Up to VO-Manager and Atlas-CSIRT 2.5 h with with DN of PJS.
  - Heads-Up to UK CA (PJS-Cert) not done, instead communication via VO-Manager, OK



- Containment:
  - Job stopped within 1h
  - PJU banned on CEs, Not banned on WMS, SEs (smadpm), Operational problem, meanwhile addressed.
  - PJS banning/unbanning not done, communicated the issue with atlas-csirt. Situation cleared: 7h



- Forensics:
  - UI and WMS CERTS notified.
  - Network logs provided, irc/ssl mentioned.
  - job daemonizes, details on irc commands.

SSC4 results: FZK-LCG2 (KIT), Talk 17.09. 9:30

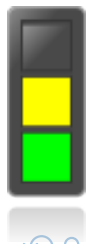
- Communication:
  - Heads-Up to EGI-CSIRT 15 min.
  - Heads-Up to VO-Manager 2h with info: suspicious irc-bot **and** User:CN=Sander Klous (SSC 4)
  - Notification to PJU-CA a bit late.
  - Timestamp of Update used, contained all relevant info.
- Containment:
  - All malicious jobs stopped after 30 min.
  - PJU banned after 30 min. cream-CE missed (took 4h) operational problem, solved already.
  - PJS banned/unbanned in time although PJU already identified within 2h.
- Forensics:
  - All tasks done within 4h + the only team that spotted PJU banning monitor.



SSC4 results: IN2P3-CC

- Communication:
  - SSC4 preparation activity was spotted at the site already a month early 03/05/10 19:30!: *there is a job ..., using no CPU. Can I kill it? The processes for it are listed below..... ./lutra_Linux_64_rh5*
  - EGI-CSIRT, Atlas-VO and CAs informed.
  - (Good!) Update send after 21.5h, used as Final Report timestamp.
- Containment:
  - Malicious Jobs stopped (1.5h)
  - PJS and PJU banned within 1h
  - Unbanning PJS done? Panda-logs unclear.
- Forensics:
  - UI at Nikhef not found.
  - Details on binary send in (late) final report (480h)

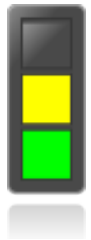




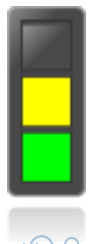
SSC4 results: INFN-T1

- Communication:
  - Heads-Up to EGI-CSIRT 1h
  - Heads-Up to VO-Manager 2h, PJS **and** PJU mentioned, asked when PJS can be unbanned again!
  - Also contacted abuse.at.hoster wunderbar.geenstijl

- Containment:
  - Malicious job stopped 2h.
  - PJS banned 3h, PJU banning at some CEs not succeeded (Operational problem?)
  - Unbanning PJS late, although asked VO-Manager, when to unban (see above).



- Forensics:
  - UI and VO-WMS found, Certs contacted.
  - HTTP traffic found, IRC/SSL protocol not found.

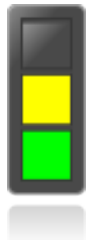


SSC4 results: Nikhef, rerun evaluated

- Communication:
  - Internal mail to security.at.nikhef coordinated the activities.
  - Heads-Up to EGI-CSIRT 0.5h, also saying WN got disconnected from the network.
  - Heads-Up to Atlas-CSIRT, first/final very detailed report 3h. *... is local to Nikhef...No further information regarding actions with respect this user will be disclosed.*
- Containment:
  - Malicious job stopped 1.5h, Panda ID send to EGI-CSIRT.
  - PJS banned 3h, unbanned 6h.
  - PJU banned at CEs 3h, WMS 6h, Ops. problem, solved.
- Forensics:
  - All involved hosts (incl. my laptop) found, Certs informed
  - ...irc bot maintained an open TCP connection port 25443..hosts at CERN, BNL involved
  - List of involved mechanisms Globus Tool kit 4 Gatekeeper, Condor - Condor-G job management for

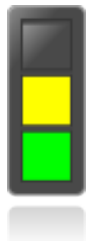
SSC4 results: PIC

- Communication:
  - Heads-Up to EGI-CSIRT 1.5h DN: graeme andrew stewart (ssc4)
  - Heads-Up to VO-Manager 1.5h DN: graeme andrew stewart (ssc4)
  - No communication to CA
  - No Final Report



- Containment:
  - Angel quit 1.5h, Daemon 11h "*and also killed the job.*" (Artefact?)
  - PJS banned 2.5h, unbanning not done
  - PJU not found/mentioned

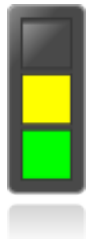
- Forensics:
  - VO-WMS found, UI at Nikhef not mentioned
  - "Only" irc Connection found.
  - irc commands in binary found, cron, at daemonizing not mentioned



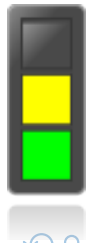
SSC4 results: Prague-LCG2

- Communication:
  - Heads-Up to EGI-CSIRT 1h
  - CA and VO not contacted, security contact wanted to limit communication to training address.
  - Update used as Final Report.

- Containment:
  - Malicious job stopped 30 min.
  - PJS banned 7h.
  - PJU shows up in log excerpt as well as the panda url, info **not** used $user = Sander\%20Klous\%20SSC4\&days = 3$
  - PJS not unbanned

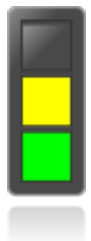
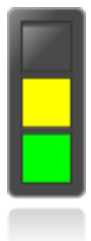


- Forensics:
  - VO-WMS found, UI at Nikhef not mentioned
  - IRC over SSL found, no further info.
  - irc found, cron/at attempts spotted, gridssh not mentioned; strings, shasum send,



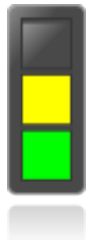
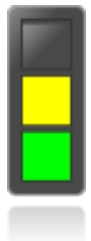
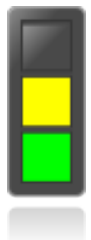
SSC4 results: RAL-LCG2, Run-2 new local CERT member

- Communication:
  - Heads-Up, Alarm mail acknowledgement 2h
  - Heads-Up to VO-Manager: banned PJS,PJU 5.5h
  - Dutch and UK Grid CA notified 5h
  - Final Report 120h contained Info that was needed earlier
- Containment:
  - Malicious job stopped 6h
  - Banning PJS 8.5h
  - PJU Banning missed at WMS
  - unbanning PJS 9h
- Forensics:
  - All forensic only in final report 120h.
  - VO-WMS and UI at Nikhef found.
  - irc over ssl, gridssc.sh, strings against lutra in final report

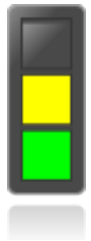
SSC4 results: RRC-KI

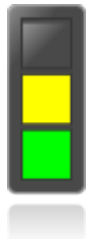
- Communication:
  - Heads-Up to EGI-CSIRT 6h, Nikhef notified earlier
  - Heads-Up to VO-Manager 6h: panda ID and IRC activity.
  - CAs not notified.
  - Initial report complete, atlas-adc-central-services@cern.ch was not responding (solved, wrong address)
- Containment:
  - Malicious job, SSC4 monitor (55h) not reliable when connection is dropped.
  - PJS banned 5.5h unbanning after 24h, monitor problem?
  - PJU only banned on one CE.
- Forensics:
  - Found VO-WMS, UI at nikhef missed, check panda-job id.
  - Network: SSL/IRC runs InspIRCd, connects to *:25443
  - Binary: gridssc.sh, lutra (daemonizing, irc client, cron)
  - Provided script to check wunderbar for active clients

SSC4 results: SARA

- Communication:
  - Heads-Up to EGI-CSIRT 1h
  - Heads-Up to VO-Manager, with: graeme andrew stewart (ssc4)
  - Heads-Up only to Dutch CA.
  - Several follow ups send, no final report.
- Containment:
  - Malicious job killed 2h
  - PJS banned 3.h, unbanning not done.
  - PJU banned on CEs, SEs, WMS missed
- Forensics:
  - VO-WMS found, UI at nikhef not found.
  - Key feature (irc) not mentioned.





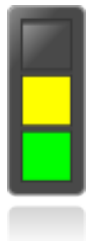
SSC4 results: Taiwan-LCG2

- Communication:
  - Time zone problem, ssc4-start times set to 9:00 local.
  - Heads-Up EGI-CSIRT 3h.
  - Heads-Up VO-Manager 12h. Confusing first report.
  - Final Report: some information missing.
- Containment:
  - Malicious job stopped 6h.
  - PJS banned 11h
  - PJU communicated by Atlas-CERT (Graeme), banned 24h
  - PJS unbanned 33h
- Forensics:
  - VO-WMS and UI at Nikhef found, Nikhef not notified.
  - Network: lutra to *: 25443 ssl/irc not mentioned.
  - Binary: grdissc.sh described, lutra not, executed on some host, provided a tar ball with input sandbox



SSC4 results: Weizmann-LCG2

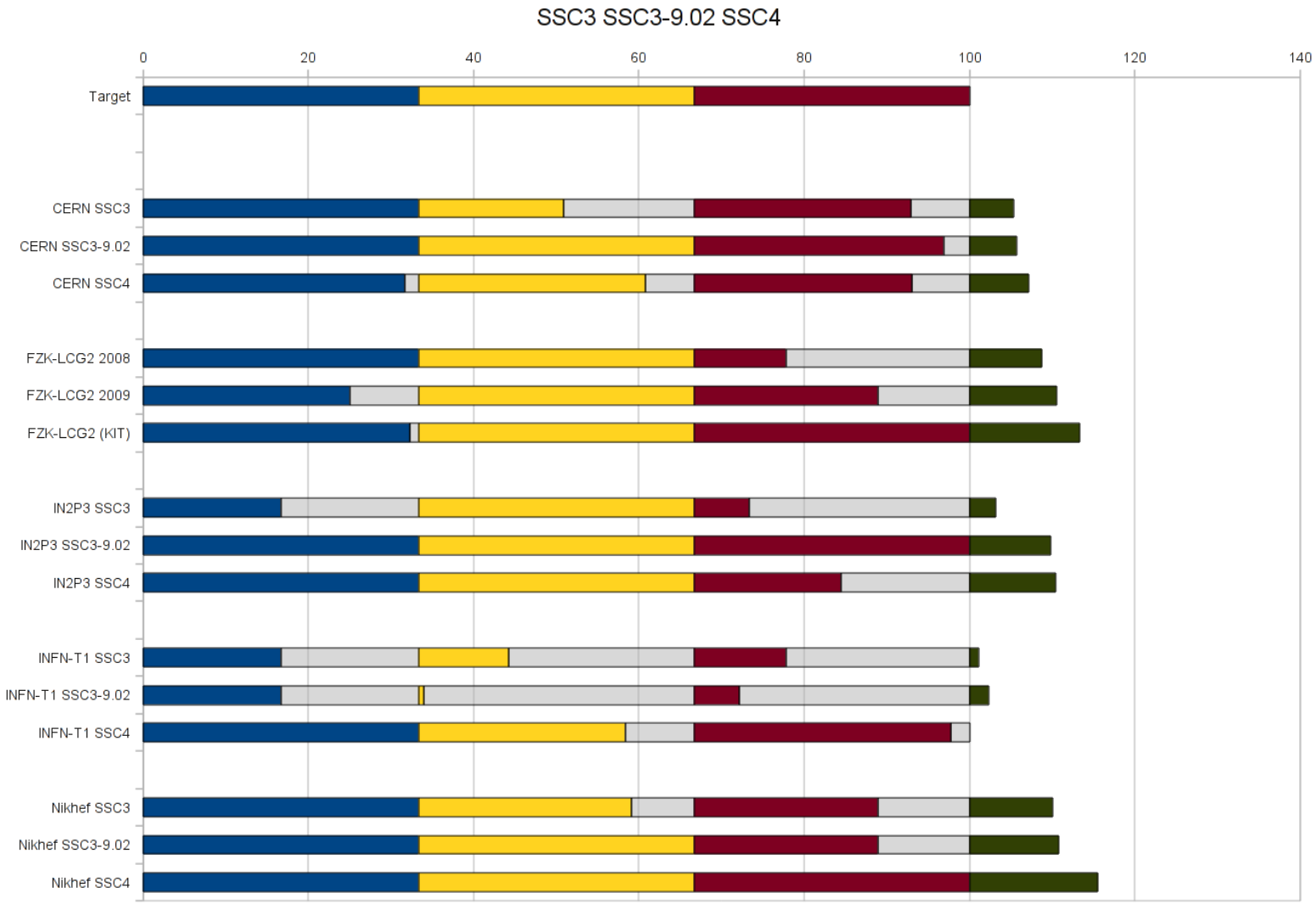
- Communication:
  - Heads-Up to EGI-CSIRT 3.5h.
  - Heads-Up to VO-Managers 6h PJS, voatlas61.cern.ch, lutra_Linux_64_rh5.
  - Heads-UP to UK-CA (PJS) activity described.
  - Final report not complete.



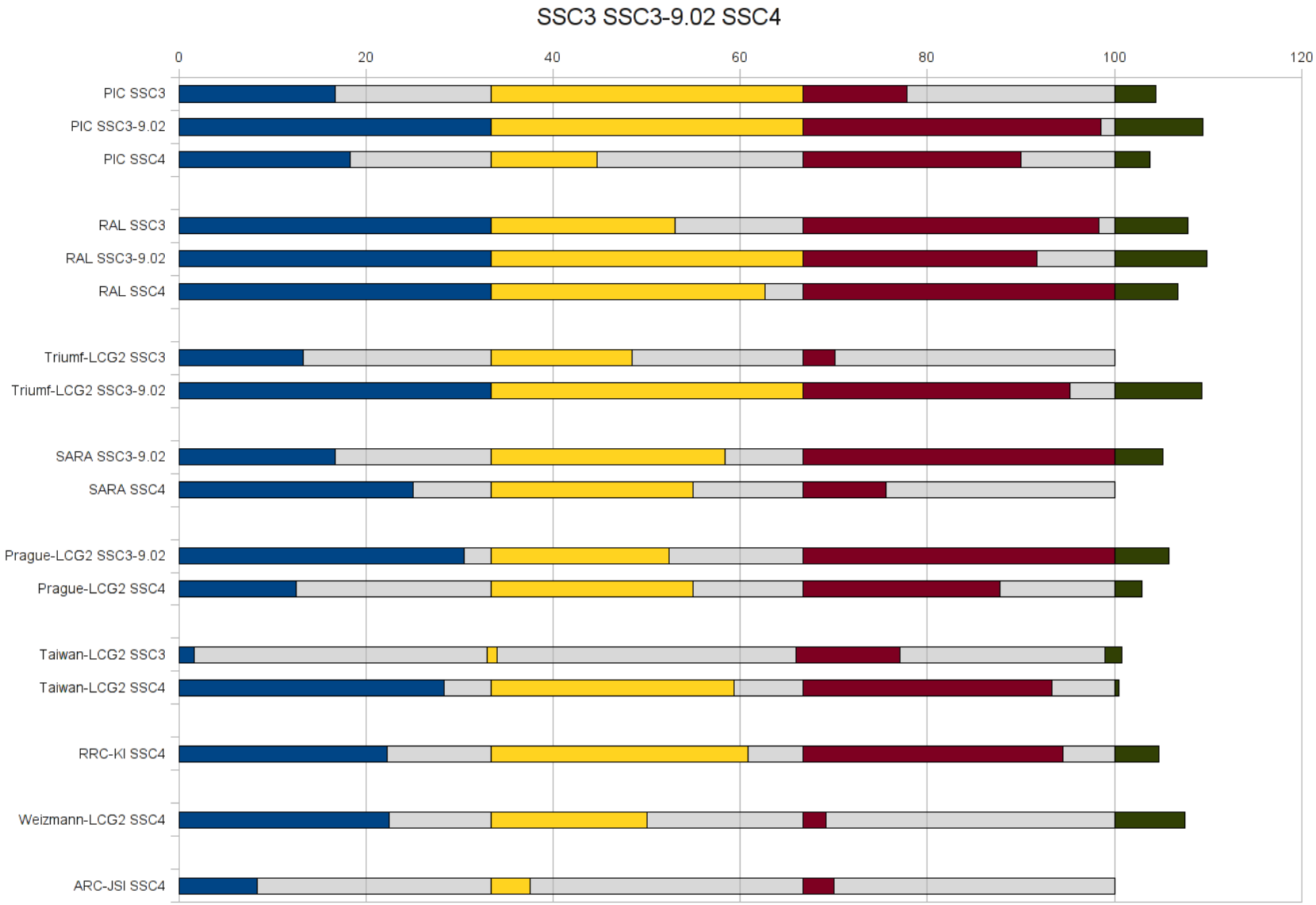
- Containment:
  - Malicious Job killed 2.5h
  - PJS banned 6h.
  - PJU not mentioned not banned.
  - PJS Not unbanned.

- Forensics:
  - VO-WMS found, UI at Nikhef not mentioned.

Results SSC3 / SSC4



Results SSC3 / SSC4



Summary

- Communication
  - improved a lot. All sites send Heads-Up in time.
  - Mail format/content improved. Problems with close out report, communicating to CA
- Containment:
  - Some sites have user management problems.
  - Second DN not found by all sites, banning/unbanning to be improved.
  - Available info not used (Panda-ID, URL).
- Forensics:
  - User-Interface not found by all sites
  - Forensics Network and ”malicious binary’ to be improved.
  - Technical skills do vary a lot, collaboration to be addressed in next run.
- Atlas-Debriefing: http://indico.cern.ch/conferenceDisplay.py?confId=83604

Summary

User/Grid-Certificate Management

	React. time *h*		Grid-Certificat Management	
Drill	Heads-Up	Stop Procs	Success %	Time *h*
SSC-3 2008	2.6	6.8	66	5.5
SSC-3 2009	1.4	1.8	100	1.5
SSC-4 2010	1.2	3.2	100(PJS)/ 75(PJU)	4.7 (PJS)/6.8 (PJU)

- PJS banning only monitored at CE, problem with managing cerificates at multiple services, multiple certificates associated with one job.
- ”Banning-process” itself is not more complicated than other config-file based operations.
- Problem: no success-control of the operation possible.
- might point to operational problems with the Fabric Management
- might be worse at smaller sites.
- Central Certificate Management might improve the situation.

NGI-Runs/Projekt-wide Run

- Run in NDGF. Run in NGIs.
- Scope/Evaluation standardised/automated.
- Monitor sites security operations with tools provided (ticketing system).
- Include storage operations.
- Address colaboration between Site-CSIRTs on project level.

EGI-CSIRT operations SIG (L. Nixon))/RT-IR (C. Bermejo)

- EGI-CSIRT OS-VA started in March 2010 (one person), now focus on OS-vulnerability detection
- VA in SVG needs high quality input
- Semi informal group now invites new members having a background in discovering OS-Vulnerabilities
- Goal: Collect/process information from various public and non-public information sources to issue early warnings about likely upcoming security problems to EGI security groups and other stakeholders.
- This information could then be used in SVG and further processed in a Vulnerability Assessment procedure.

EGI-CSIRT operations SIG (L. Nixon))/RT-IR (C. Bermejo)

- Follow up with sites on Incidents as well as with Advisories/Recommendations on certain CVEs not efficiently doable by mailing (history/statistcs)
- RT-IR, issue tracker/ticketing-system for Incident-Response
- Add-On to existing RT (EGI)
- Principle set-up done, Adapting to our needs in progress (queues message templates etc)
- Interfacing with Monitoring/GoC-DB (Contact addresses) in progress
- expertise on this system available within EGI-CSIRT (Carlos)