Security Service Challenges

testing our incident response capabilities

Sven Gabriel, Nikhef

www.eu-egee.org

e-infrastructure

Information Society and media

CAPACITIES

Motivation

- Mingchao's talk (Security Training 23. Sept.).
- Professional interests in resources.
  http://cern.ch/osct/docs/egee07-r.mollon-grid.and.security.pdf
- Check your log files for "dictionary attacks"

  Illegal users from these:
  admin/none from 85.17.145.99: 18 Time(s)
  anda/none from 85.17.145.99: 2 Time(s)

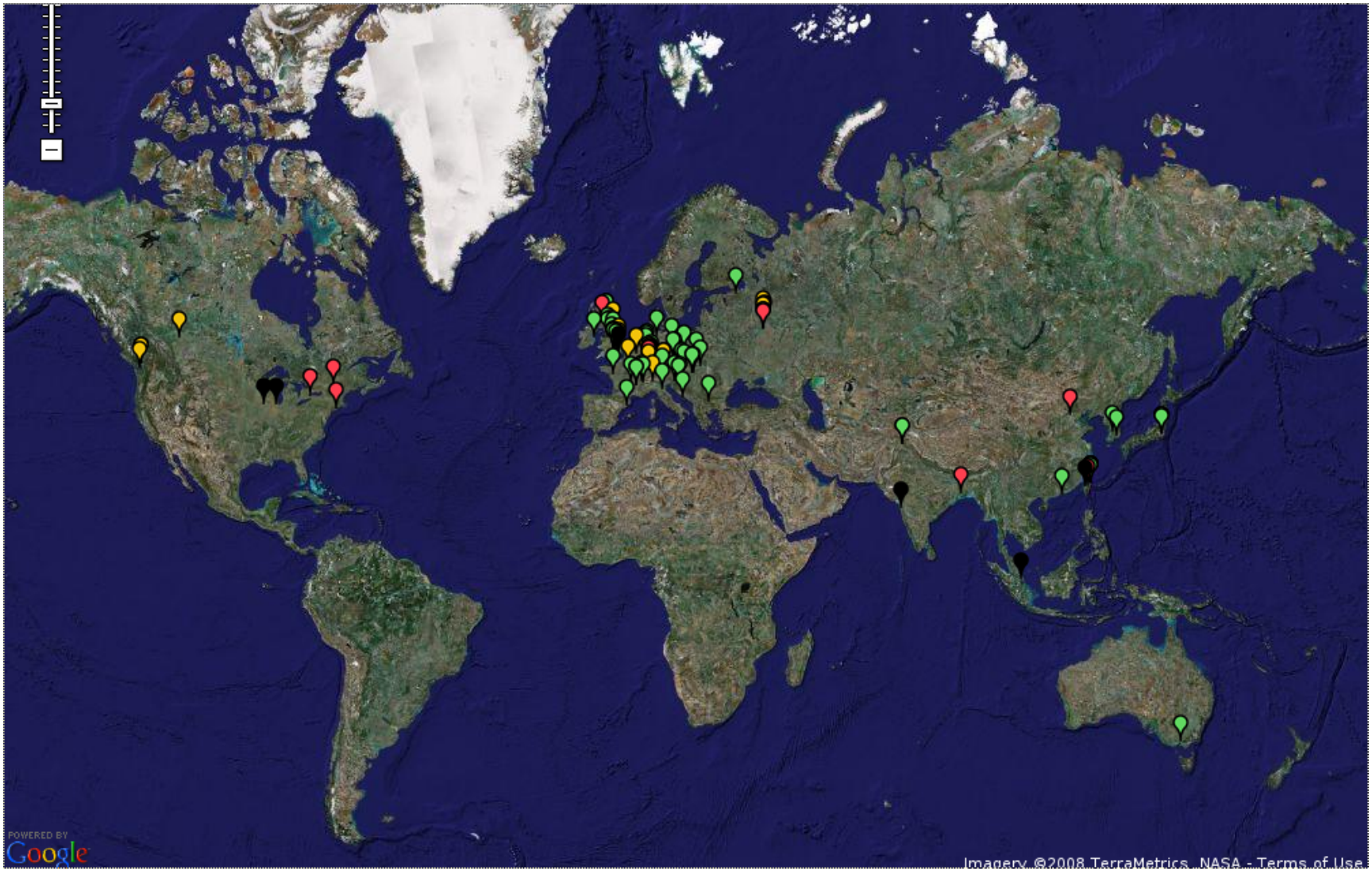
Site Security, General Remarks

- Sites “attached to a Computing Center” will have security/fabric-management tools in place.
- Ensure communication channels with the involved admins are in place.
- New Sites without a supporting Computing Center:
  - Plan Network-layout carefully.
  - Secure communication with your hosts -ssh with password protected keys
  - Fabric-Management-Tool - updates / patches - effectively react on incidents like ban users.
  - Central-Syslog with automatic parsing of logfiles
  - Security-Monitoring -filesystem integrity -network analyzer
- Security Workshop -this conference
- http://osct.web.cern.ch/osct/dissemination.html

The objective:

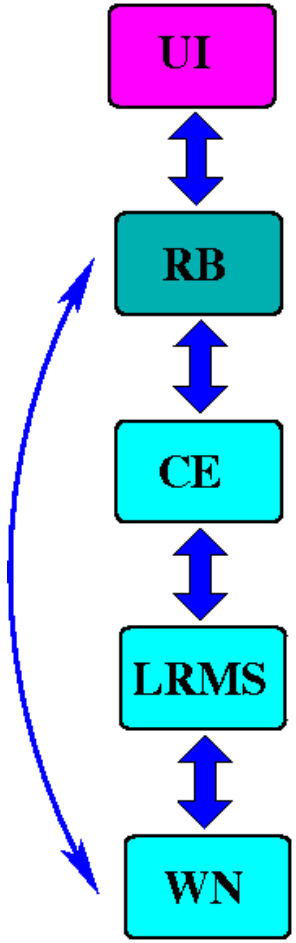
The goal of the LCG/EGEE Security Service Challenge, is to investigate whether sufficient information is available to be able conduct an audit trace as part of an incident response, and to ensure that appropriate communications channels are available.

SSC -Objective



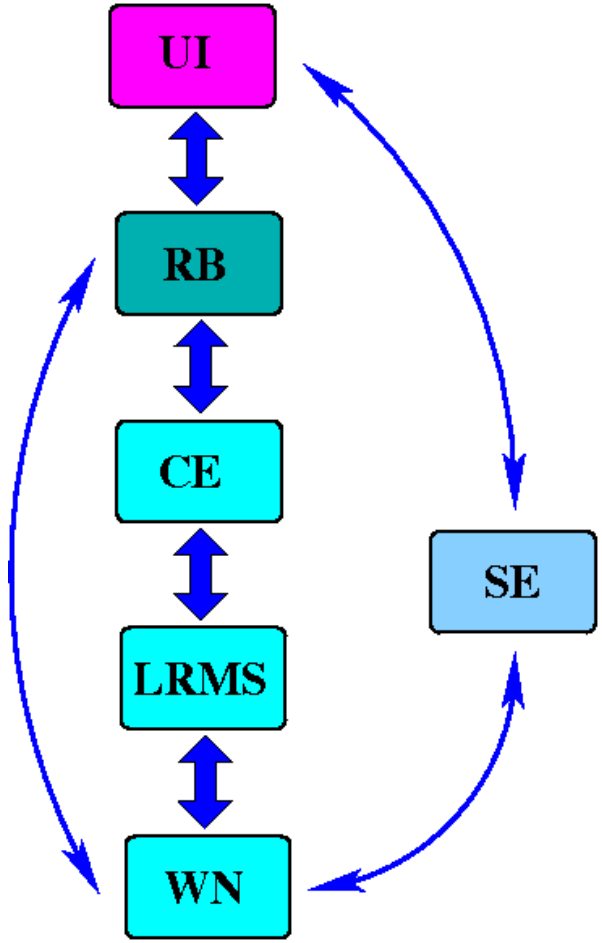
Security Service Challenge

- Connecting 290+ sites with Grid-Middleware.
- Involved services per job are in general distributed.
- Jobflow, easily 3/4 sites involved.
- To get a complete picture the communication channels to all sites have to work.
- Syslog not always used by the Middleware
- Several logfiles (locations) have to be parsed.



Security Service Challenge

- Connecting 290+ sites with Grid-Middleware.
- Involved services per job are in general distributed.
- Jobflow, easily 3/4 sites involved.
- To get a complete picture the communication channels to all sites have to work.
- Syslog not always used by the Middleware
- Several logfiles (locations) have to be parsed.



SSC Common Setup

- SSCs were run in two stages:
  - Stage 1: targeting the principal sites in the regions
  - Stage 2: targeting the individual Sites in each ROC
- The jobs were submitted from an User Interface (UI) to a chosen Grid Compute Element (CE) via a Resource Broker (RB) using standard Grid commands
- They consist of a set of small, non-intrusive programs.
- Not intrusive, only 'legal' operations are executed (jobsubmission, file transfer, ...)
- No penetration tests, no execution of exploits etc.

SSC Common Setup

- SSC-1 (2005 – March 2006) targeted the Workload Management System (WMS): Resource Broker (RB) and Compute Element (CE).
- It tested whether sufficient information was available and whether communication channels were sufficiently open
- Did not address the Security Incident Response Procedure
- Used Savannah as the vehicle for communication between the Test Operator (TOP) and the Target sites.

SSC-1 - Task

- Given: Time range, IP-address of the target computer, UNIX-UID of challenging job on target
- The Sites had to find out:
  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?

SSC-1 Results - Findings I

- Nr. of challenged sites
  - 129 (out of a total of 190) participating Grid Sites have been challenged.
- Response
  - Some Sites did not respond to the alert. Security Contact list outdated, Security Contact overloaded, or the initial e-mail of the alert got lost or was thrown away....
- Feedback
  - Respondents esteemed the level of difficulty to be about right.
  - 2 – 3 people involved, response times varied from 2 to 363h (SSC-1 had not been announced as a high priority test)
  - Several sites got a little confused by the time stamps on the alert. TOP used UTC consistently in all communication. This was not sufficiently explicit, so one site got severely de-railed by time-skew at first.

SSC-1 Results - Findings II

- A relatively heavy workload fell on the shoulders of the system administrators of the Resource Brokers (RB). Most ROCs would submit the challenges via a small selection of RBs.
- The retention period for log files was not sufficiently long on all sites.
- Additional Tools (Centralized Logger) needed to optimize the access to the needed information at sites.
- Full debriefing report:
  - https://twiki.cern.ch/twiki/pub/LCG/SSC1/SSC_1_Debrief_2006-04-18.pdf
  - https://twiki.cern.ch/twiki/pub/LCG/SSC1/DebriefRecommend.pdf

SSC-2 Objective and Setup

- SSC-2 tested the traceability of storage operations (2007).
- From the Worker Node (WN) a sequence of seven storage operations have been executed.
- Did not address the Security Incident Response Procedure
- Used the Global Grid User Support (GGUS) as the vehicle for communication between the Test Operator and the Target Sites.

SSC-2 - Task

- Given: User DN, Time range and SE
- The Sites had to find out:
  1. For each of the identified storage operation, please indicate:
     - The exact time (UTC).
     - The type of operation.
     - The URLs, filenames, catalog names and filepaths involved.
  2. Please indicate the IP-address of the User Interface (UI) that was used for the Job Submission?

SSC-2 Results - Findings

- Response
  - From the Test Operator's (TOP) point of view, the challenged ROCs had the GGUS ticket routing set up with sufficient precision to direct the ticket to the appropriate service.
  - All the challenged ROCs responded to their alert.
  - The TOP identified the "in Progress" state of the ticket as the acknowledgment. The TOP never had to escalate the ticket and did not intervene in the ticket routing.
  - Not all tasks of SSC-2 could be solved, since the logging of the middleware was not cabable to provide the needed information. Feedback was sent to the developers. SSC2 should be rerun.
- Feedback
  - Majority found the difficulties as expected and appropriate.
- Full debriefing report:
  http://grid-deployment.web.cern.ch/grid-deployment/ssc/SSC_2/Stage_1/debriefingReport.html

SSC-3 Objective and Setup

- SSC-3 -a more realistic simulation of an incident, it challenges the Operational Responsiveness of LCG/EGEE Grid Sites.
- The Job is launched from a User Interface (UI);
  - It runs with valid credentials.
  - Once running, it will exploit its environment to conceal its activities.
  - Sign of life will be reported through an out-of-band channel.

SSC-3 Objective and Setup II

Alert

- The Alert is sent to the CSIRT e-mail address registered in the Grid Operations Center Data Base (GOCDB).
  - The text clearly identifies the alert as a test.
  - The Grid identity of the submitting user is indicated.
  - The Site is asked to deal with the Alert following approved Incident Response Procedures.
  - However, an alternative e-mail address is indicated to replace the normal multi-destination addresses.

SSC-3 - Incidence Response

The Incident Response is broken up in three activities:

- Communication
  - Acknowledgment/Heads-up report to the indicated e-mail address.
  - Alert to the VO manager.
  - Verification that the responsible Certification authority has been notified.
  - Filing of the final report.
- Containment
  - Identification of the Job and killing of its processes.
  - Suspension of the offending user at the challenged Site.
- Forensics
  - Discovery of emitting Site and contact to the Sites CSIRT.
  - Analysis of network traffic.
  - Analysis of the submitted binaries.

SSC-3 - Evaluation

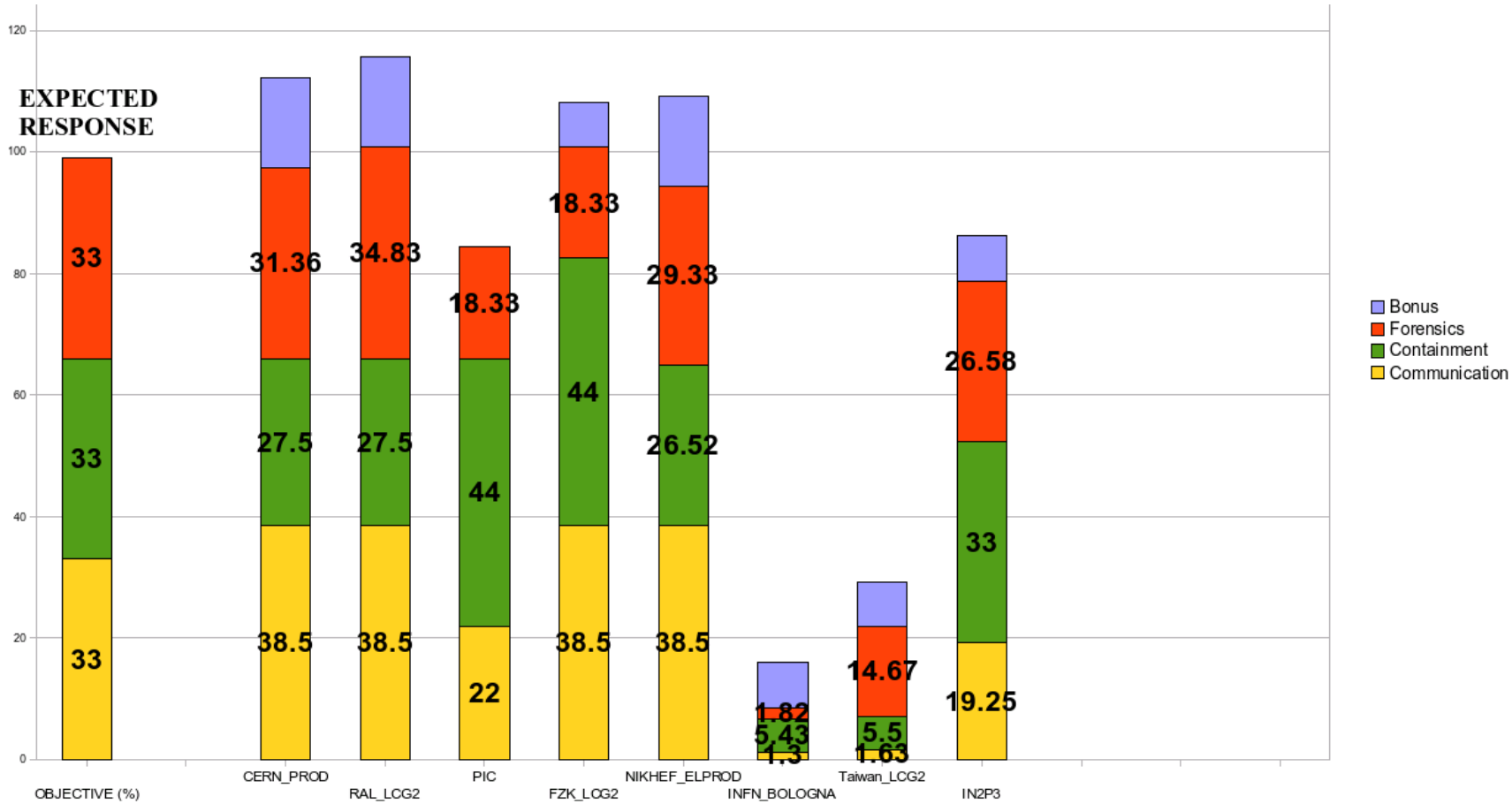
The challenged Sites response will be evaluated by OSCT

- For the completeness and timelines in terms of:
  - Filing and distribution of the reports.
  - Alerting of the cooperating bodies.
- For the demonstrated technical abilities:
  - To disentangle the Job.
  - To execute managerial tasks on Grid elements.
  - To preserve and analyze the evidence.

SSC-3 Results - Findings

- Not all malicious processes have been killed
- Suspending User incomplete (only on local RB).
- Analysis of the network traffic incomplete / malicious offsite network traffic not detected.
- Incomplete communication and forensic reports.
- In one case only little information received and little action taken.
- ≈ 1/3 of the Tier1s unable to block the malicious DN. Discrepancy to the reported level of difficulty of the tasks.
- ≈ 2/3 of the Tier1s unable to kill the malicious processes.
- Only 1 site killed all malicious processes without unplugging the WN.

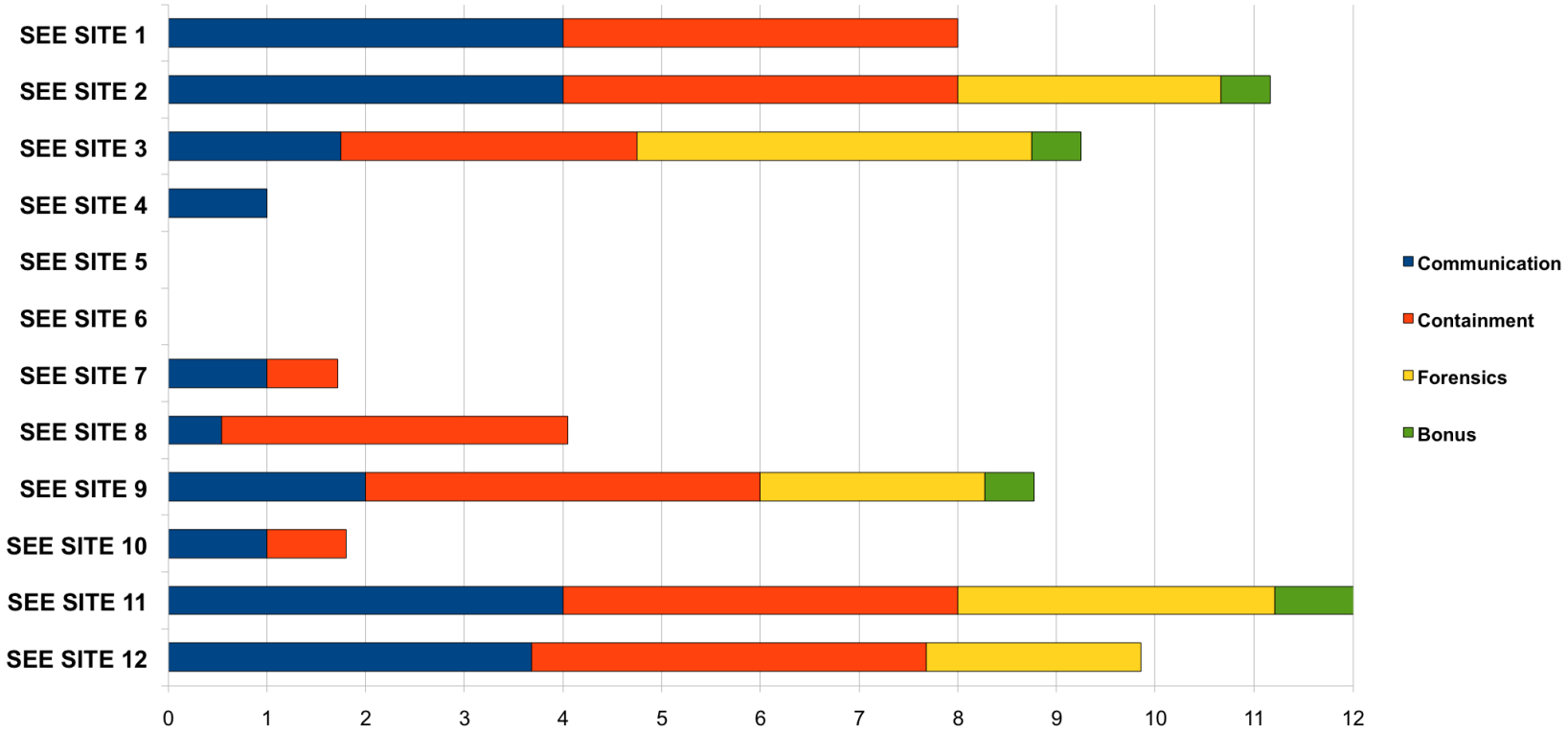
SSC-3 Scores (Normalized, Romain)



SSC-3 Results ROC-SEE, Christos

- Incorrect Site's CSIRT contact details. (alert email was sent back with No such usermessage from mailer daemon), alert got stuck in a SPAM-Filter
- Not all Site's admins/security contacts are familiar with the security incident procedure, didn't know how to trace back the UI.
- Problems doing the forensics properly (binary as well as network analysis).

SSC-3 Scores ROC-SEE, Christos



Summary Findings

- Since the involved services in a Grid-Job are distributed, it is crucial to have comparable security expertise on all sites.
- Every site must be able to find the needed information to trace a job and to ban a user.
- $\approx$ 1/3 of the Tier1s unable to block the malicious DN. Discrepancy to the reported level of difficulty of the tasks.
- $\approx$ 2/3 of the Tier1s unable to kill the malicious processes.
- one site did not react/mail lost.
- Incident response procedure generally understood.

Summary SSC-Feedback

- To run SSCs require some effort by OSCT. All sites have to give the SSCs a certain priority to make optimal use from them.
- SSC-Feedback
  - Better tools to ban a user needed.
  - Logging is often a problem: middleware logs, lack of central syslog. LB-Talk Daniel Security Training Session need to optimize the access to the needed information to track a job. Use syslog (SSC-1, March 2006).
  - Better security procedures are needed for the sites. Could be done by using the SSC-Results (Carlos talk Security Training Session -Review your Procedures).

SSC-3 Next Discussion Questions

- Next:
  - Rerun SSCs to check if the feedback is implemented (SSC-2 Storage).
  - Rerun SSCs to update/improve procedures
  - New SSCs needed to address new services, more realistic simulation of the reality.
- Thanks: Romain, Pal, Christos, Daniel and Ursula.