Security Challenges in Distributed Environments

Sven Gabriel, sveng@nikhef.nl
Nikhef http://nikhef.nl EGI-CSIRT http://egi.eu

Leif Nixon, nixon@nsc.liu.se
NSC/SNIC/NDGF/EGI-CSIRT http://egi.eu

Introduction

- EGI: European Grid Infrastructure
- EGI-CSIRT

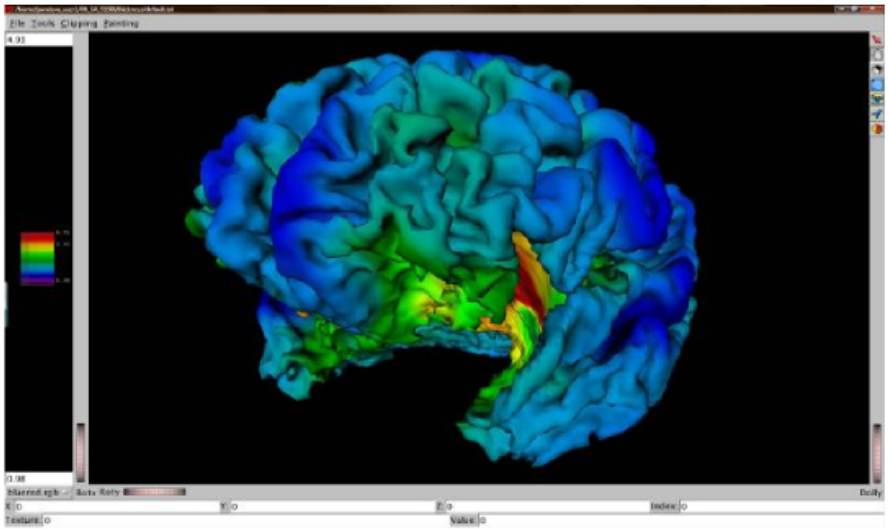
40 Sites, 20 countries, one global security exercise

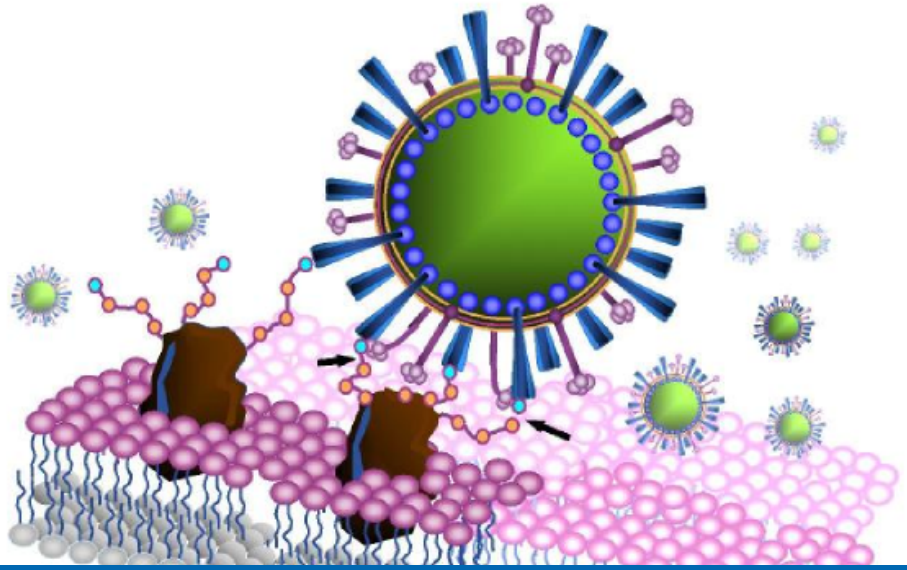
- Introduction to Security Drills in a grid infrastructure
- A Framework for global Security-Drills
- SSC-5 Security Incident involving a VO-Job-Submission Framework

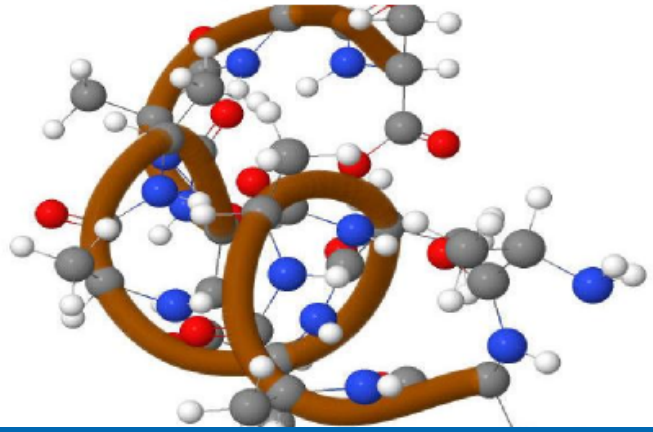
Incident Response Task Force - IRTF

- Incident Response

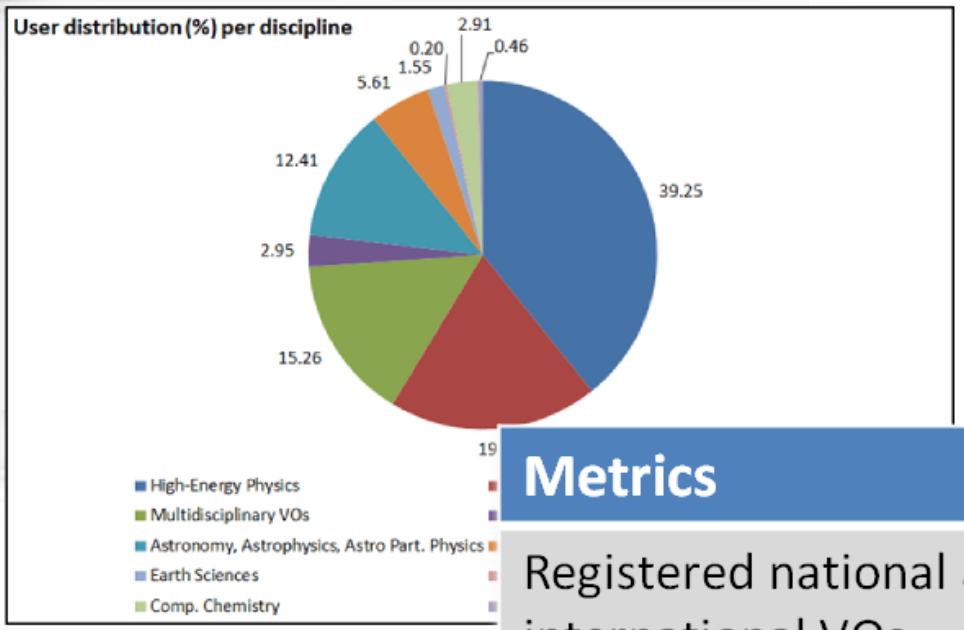
EGI some numbers







EGI some numbers



Metrics	Value (% change)
Registered national and international VOs	226 (+3.20%)
Registered users	20883 (+14.30%)
Active VOs (High/Medium/Low)	25/23/8

More heterogeneous access to the resources

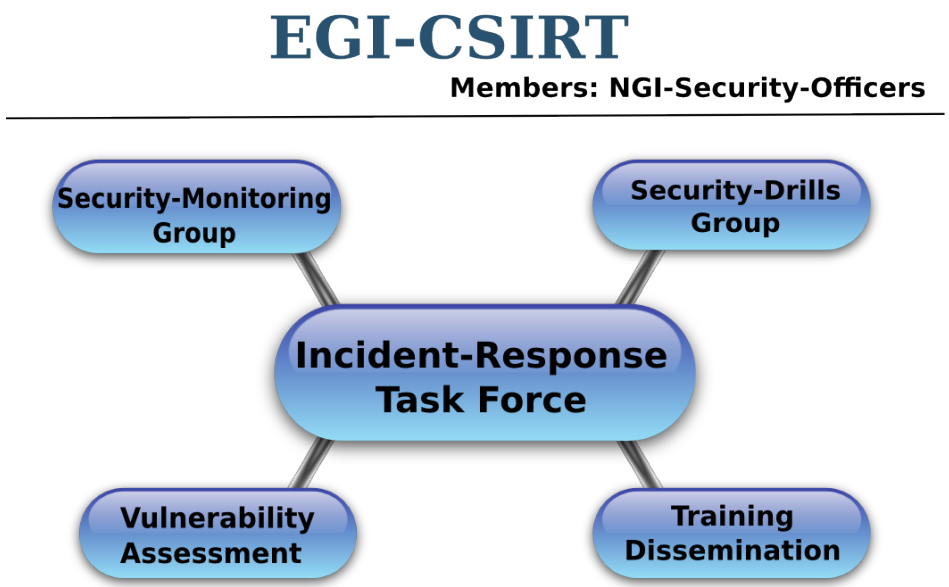
EGI-CSIRT

EGI CSIRT objective: provide the EGI infrastructure with incident response capabilities across the participating NGIs.

EGI-CSIRT

EGI CSIRT objective: provide the EGI infrastructure with incident response capabilities across the participating NGIs.

- EGEE / EGI
  ($\approx$ 12 ROCs $\rightarrow$ 50+ NGIs)
- Project wide coordination of operational security activities.
- Interfacing to other (Grid/NREN/VO) CSIRTs
- EGI-CSIRT central tasks, security activities coordination



Trust / Accreditation TF-CSIRT

Interfacing to other (Grid/NREN/VO) CSIRTs

- Collaboration with other CERTs, share Information, **Trust**
- Describe / Document your CSIRT, operational requirements to be met
- RFC-2350
- Provided information gets evaluated.

Trust / Accreditation TF-CSIRT

Interfacing to other (Grid/NREN/VO) CSIRTs

Operational Security

Security in EGI

- Security Coordination Group (SCG), overall coordination of the security activity in EGI
- Security Policy Group
  - Agreement on Rules
  - Deal with new technologies (ex.VO-Job submission frameworks, Cloud technologies)
  - Monitor that the rules are obeyed

Operational Security

Security Operations in EGI

- In case of a *Critical Vulnerability, Advisories are set up /send to the sites.*

Operational Security

Security Operations in EGI

- In case of a *Critical Vulnerability, Advisories are set up /send to the sites.*
- *If sites don't take action, further explanations in tickets, also a clear statement, that ....*

Operational Security

Security Operations in EGI

- In case of a *Critical Vulnerability, Advisories are set up /send to the sites.*
- *If sites don't take action, further explanations in tickets, also a clear statement, that ....*
- *Failure to take the advised steps might ultimately lead to site suspension.*

Operational Security

Security in EGI, SVG I

- Security Vulnerability Group
- Eliminate existing vulnerabilities from the deployed infrastructure, primarily from the grid middleware.
- Risk Assessment Team (Middleware developers, security experts)
- Result: Risk is either Low/Moderate/High/Critical, this determines which procedure is to be followed.

Operational Security

Security in EGI, SVG II

- 70 vulnerabilities reported since started EGI Software Vulnerability handling (in Sept 2010)
- 37 Valid Distinct Grid Middleware Vulnerabilities
- 2 ‘critical’, 8 ‘High’, 8 ‘Moderate’, 21 ‘Low’
- What if you find a software vulnerability? https://wiki.egi.eu/wiki/SVG:SVG

Security Service Challenges

Security Drills / Results

Until SSC4 (2010) “per site security drills”

- Script based malware deployment.
- Evaluation based on:
  - Manually processing response mails (extracting times).
  - Digging for related information (forensics part).
  - ”malware” logs.
  - Scoring schema in a spreadsheet.
  - ... quite a human factor ... time consuming.

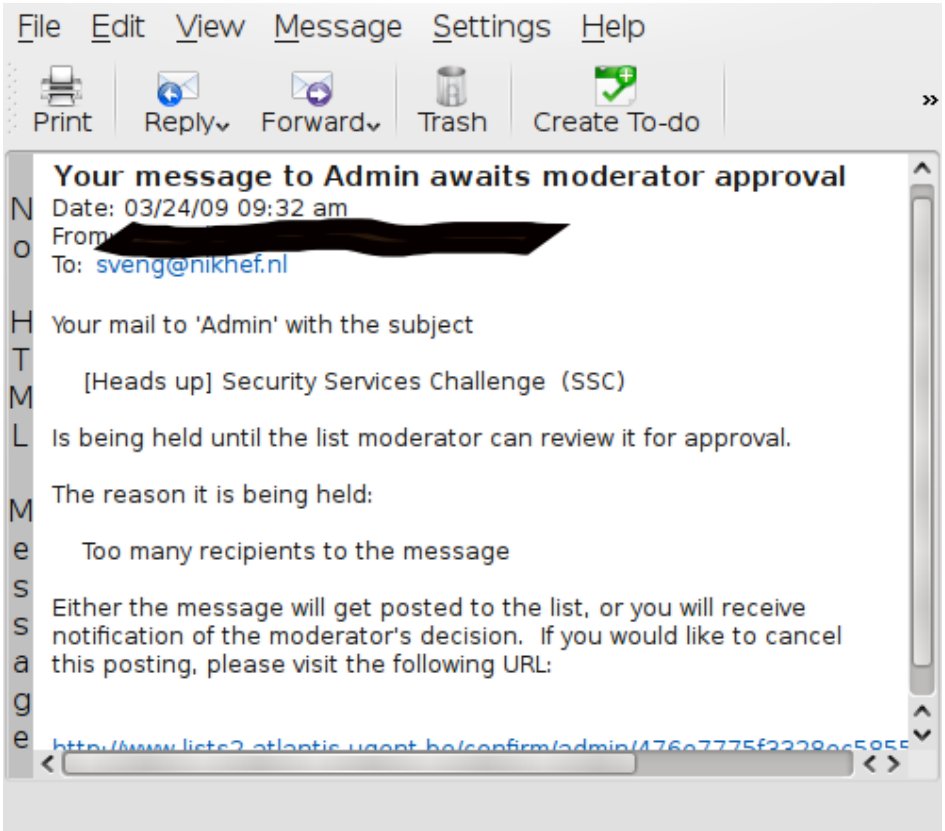
Security Drills / Results

- Communication:
  - Endpoints valid?
  - Form/Content OK ?

- Problems: Drill-Alarm ignored, contact address wrong, outdated, ...
- ....Unfortunately all the people involved in the incident response at Site XXXX were off-line on Monday ...
- .... I've received both messages. As our site YYYY does not provide any interactive access to the grid users, I developed a bad habit of not paying much attention to the security alerts.

Security Drills / Results

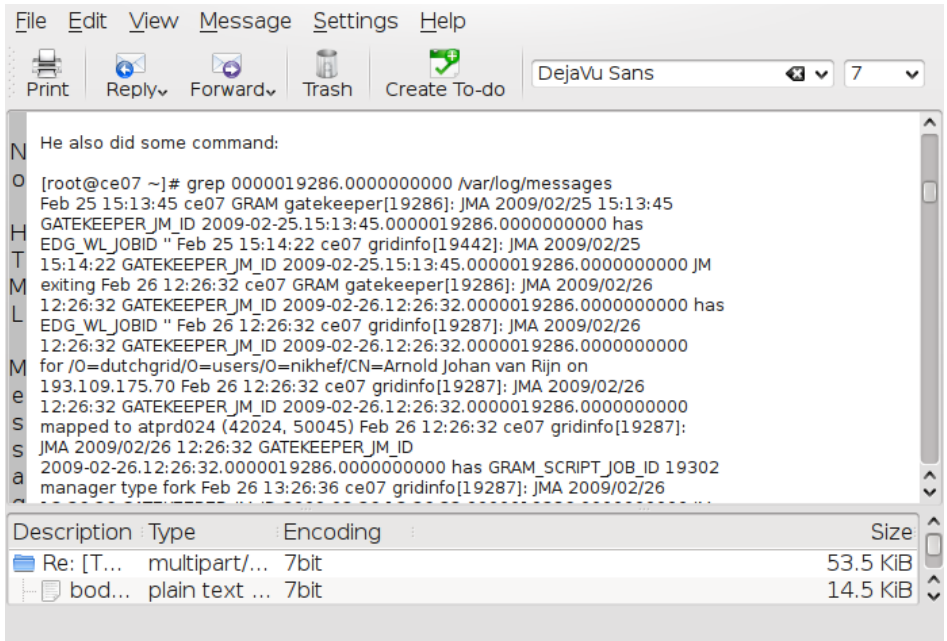
- Communication:
  - Endpoints valid?
  - Form/Content OK ?



Security Drills / Results

- Communication:
  - Endpoints valid?
  - Form/Content OK ?

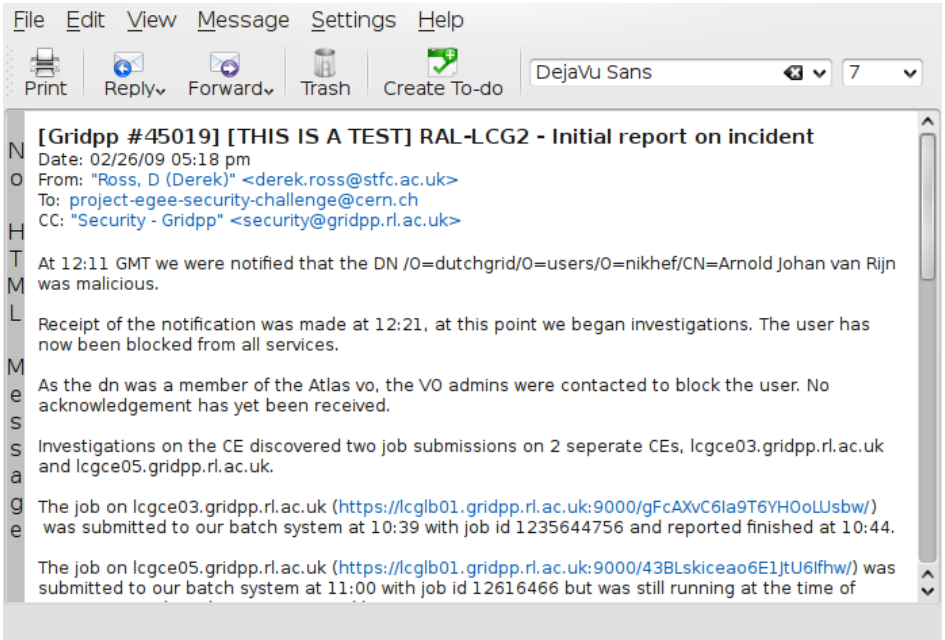
Format / Content of the received mails



Security Drills / Results

- Communication:
  - Endpoints valid?
  - Form/Content OK ?

Format / Content of the received mails



Security Drills / Results

- Communication:
  - Endpoints valid?
  - Form/Content OK ?
- Containment
  - Ban ”malicious” users
  - Find/Stop malicious processes
  - Find submission IP

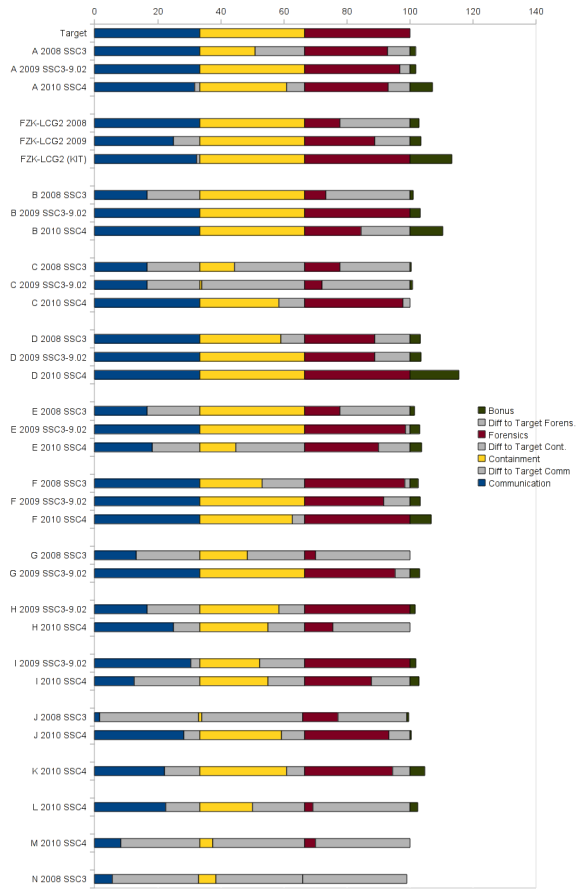
- Access Control
- X.509 based Authentication
- Definitive access control at the sites. (DN in Textfiles)
- User-certificate information gets mapped to a unix account

Security Drills / Results

- Communication:
  - Endpoints valid?
  - Form/Content OK ?
- Containment
  - Ban ”malicious” users
  - Find/Stop malicious processes
  - Find submission IP
- Forensics
  - Basic Forensics on Binary
  - Network traffic

Security Drills / Results

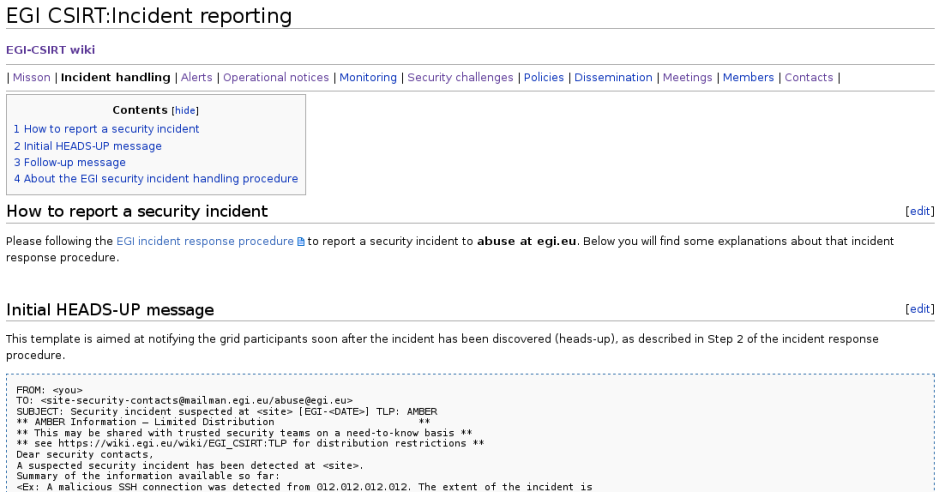
- Communication:
  - Endpoints valid?
  - Form/Content OK ?
- Containment
  - Ban ”malicious” users
  - Find/Stop malicious processes
  - Find submission IP
- Forensics
  - Basic Forensics on Binary
  - Network traffic



Sites got Supporting Material

Lessons Learned, Supporting material provided by EGI-CSIRT to the sites.

- Communication Templates



EGI CSIRT:Incident reporting

EGI-CSIRT wiki

| Misson | **Incident handling** | Alerts | Operational notices | Monitoring | Security challenges | Policies | Dissemination | Meetings | Members | Contacts |

Contents [hide]

1 How to report a security incident
2 Initial HEADS-UP message
3 Follow-up message
4 About the EGI security incident handling procedure

How to report a security incident [edit]

Please following the EGI incident response procedure to report a security incident to **abuse at egi.eu**. Below you will find some explanations about that incident response procedure.

Initial HEADS-UP message [edit]

This template is aimed at notifying the grid participants soon after the incident has been discovered (heads-up), as described in Step 2 of the incident response procedure.

```
FROM: <you>
TO: <site-security-contacts@mailman.egi.eu/abuse@egi.eu>
SUBJECT: Security incident suspected at <site> [EGI-<DATE>] TLP: AMBER
** AMBER Information – Limited Distribution                    **
** This may be shared with trusted security teams on a need-to-know basis **
** see https://wiki.egi.eu/wiki/EGI_CSIRT:TLP for distribution restrictions **
Dear security contacts,
A suspected security incident has been detected at <site>.
Summary of the information available so far:
<Ex: A malicious SSH connection was detected from 012.012.012.012. The extent of the incident is
```

Sites got Supporting Material

- Communication Templates
- Generic Incidence Response Procedure

EGI Incident Response Procedure — Site Checklist
Revision 1622 (2011-03-15)

1 – (Suspected) Discovery

1. ☐ Local Security Team — *If applicable: INFORM* ***WITHIN 4 HOURS.***
2. ☐ NGI Security Officer — *INFORM* ***WITHIN 4 HOURS.***
3. ☐ EGI CSIRT Duty Contact — *INFORM via "abuse@egi.eu"* ***WITHIN 4 HOURS.***

2 – Containment

1. ☐ Affected Hosts — *If feasible: ISOLATE as soon as possible* ***WITHIN 1 WORKING DAY.***

3 – Confirmation

1. ☐ Incident — *CONFIRM WITH YOUR LOCAL SECURITY TEAM AND/OR EGI CSIRT.*

4 – Downtime Announcement

1. ☐ Service Downtime — *If applicable: ANNOUNCE WITH REASON "SECURITY OPERATIONS IN PROGRESS"* ***WITHIN 1 WORKING DAY.***

5 – Analysis

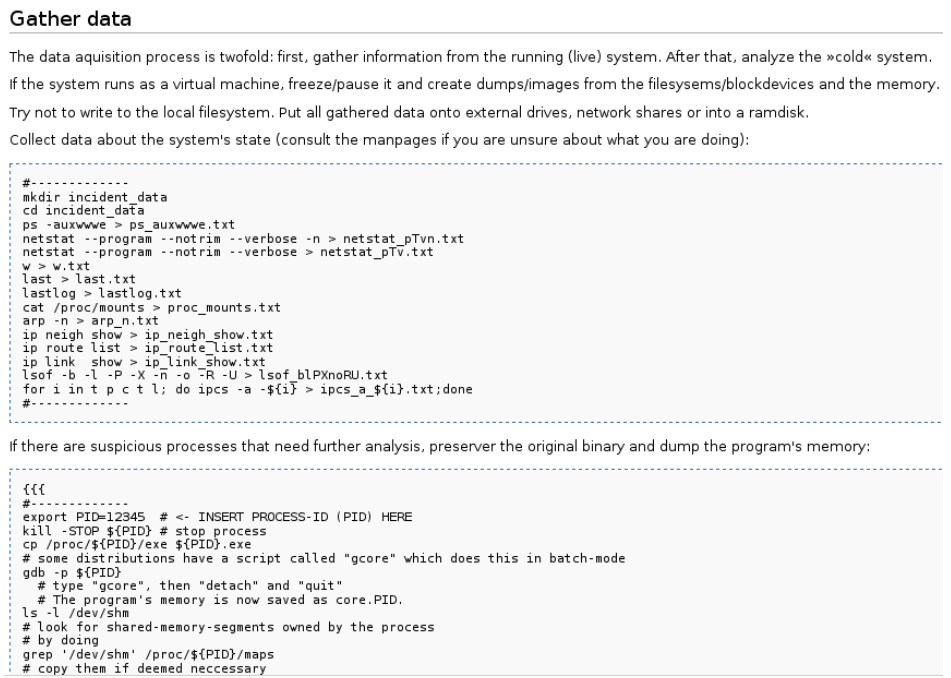
1. ☐ Evidence — *COLLECT AS APPROPRIATE.*
2. ☐ Incident Analysis — *PERFORM AS APPROPRIATE.*
3. ☐ Requests From EGI CSIRT — *FOLLOW UP* ***WITHIN 4 HOURS.***

6 – Debriefing

1. ☐ Post-Mortem Incident Report — *PREPARE AND DISTRIBUTE via "site-security-contacts@mailman.egi.eu"* ***WITHIN 1 MONTH.***

Sites got Supporting Material

- Communication Templates
- Generic Incidence Response Procedure
- Forensics guidelines



Gather data

The data aquisition process is twofold: first, gather information from the running (live) system. After that, analyze the »cold« system.

If the system runs as a virtual machine, freeze/pause it and create dumps/images from the filesysems/blockdevices and the memory.

Try not to write to the local filesystem. Put all gathered data onto external drives, network shares or into a ramdisk.

Collect data about the system's state (consult the manpages if you are unsure about what you are doing):

```
#-------------
mkdir incident_data
cd incident_data
ps -auxwwwe > ps_auxwwwe.txt
netstat --program --notrim --verbose -n > netstat_pTvn.txt
netstat --program --notrim --verbose > netstat_pTv.txt
w > w.txt
last > last.txt
lastlog > lastlog.txt
cat /proc/mounts > proc_mounts.txt
arp -n > arp_n.txt
ip neigh show > ip_neigh_show.txt
ip route list > ip_route_list.txt
ip link  show > ip_link_show.txt
lsof -b -l -P -X -n -o -R -U > lsof_blPXnoRU.txt
for i in t p c t l; do ipcs -a -${i} > ipcs_a_${i}.txt;done
#-------------
```

If there are suspicious processes that need further analysis, preserver the original binary and dump the program's memory:

```
{{{
#-------------
export PID=12345  # <- INSERT PROCESS-ID (PID) HERE
kill -STOP ${PID} # stop process
cp /proc/${PID}/exe ${PID}.exe
# some distributions have a script called "gcore" which does this in batch-mode
gdb -p ${PID}
  # type "gcore", then "detach" and "quit"
  # The program's memory is now saved as core.PID.
ls -l /dev/shm
# look for shared-memory-segments owned by the process
# by doing
grep '/dev/shm' /proc/${PID}/maps
# copy them if deemed neccessary
```

SSC-Monitor Framework

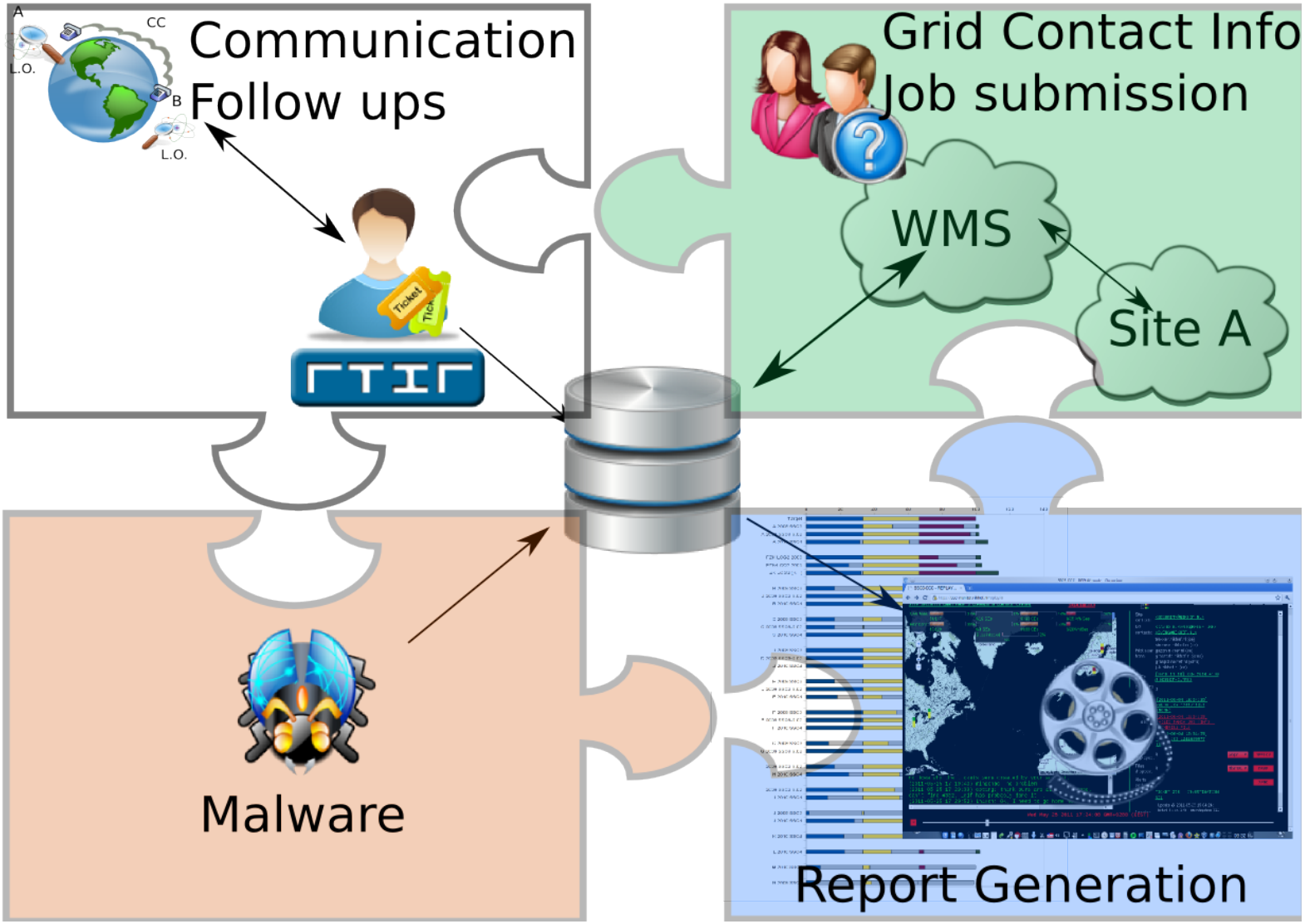
Security Drill Framework allows for:

- Various job-submission methods, Storage operations.
- Defined set of tasks (Communication, User/Process management with target times)
- Automated Report generation / Scoring schema.
- Keep history/monitor Progress.

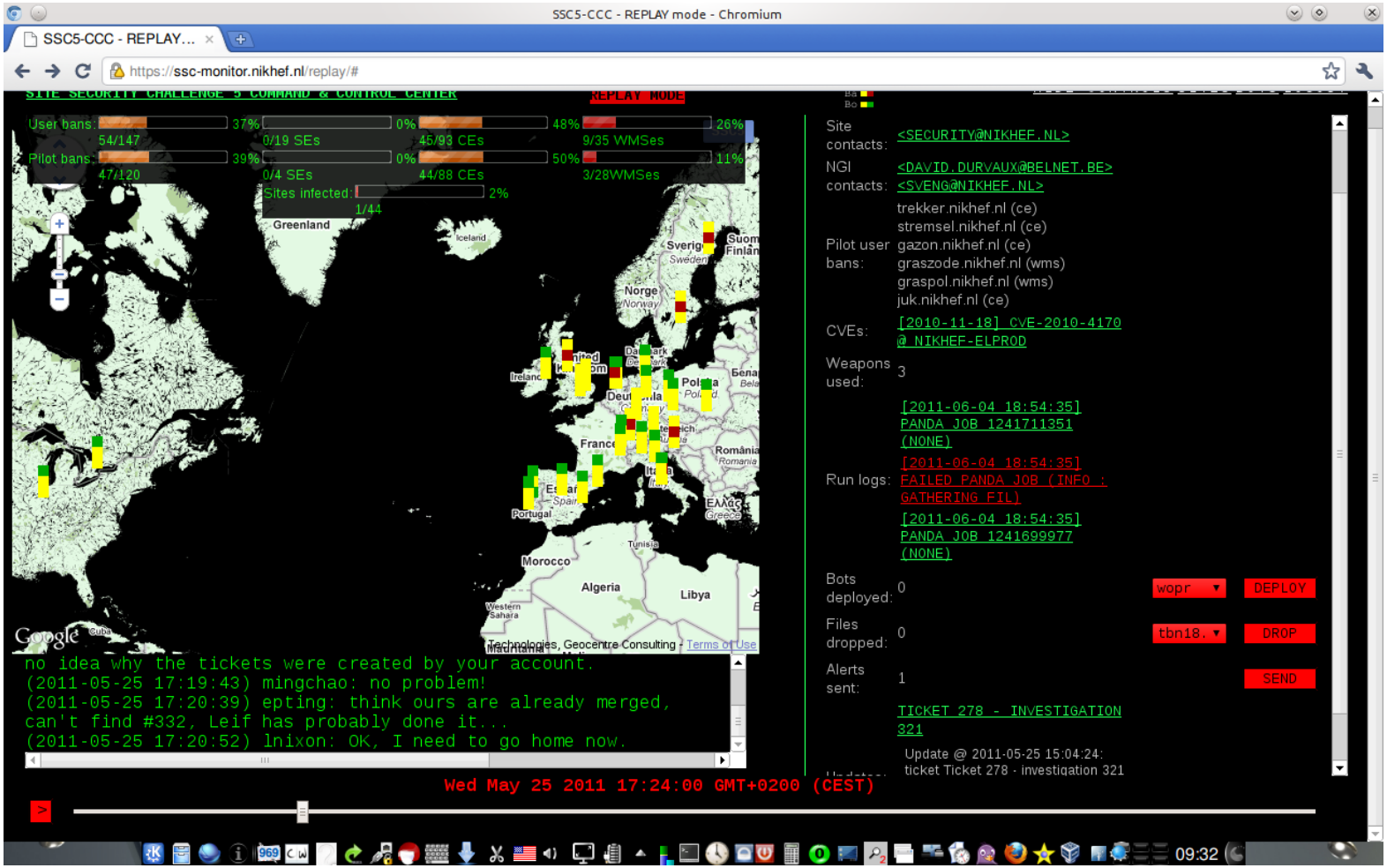
SSC-Monitor Framework

- Per site training exercise.
  - “You are on your own”, limited external information source
  - Training Site-operations, goal: improve/measure site response capabilities, procedures.
- Multi site incident simulation exercise.
  - Various information sources / focus on collaboration/information sharing

SSC-Monitor Components



48h IR in 5min



48h IR in 5 Minutes

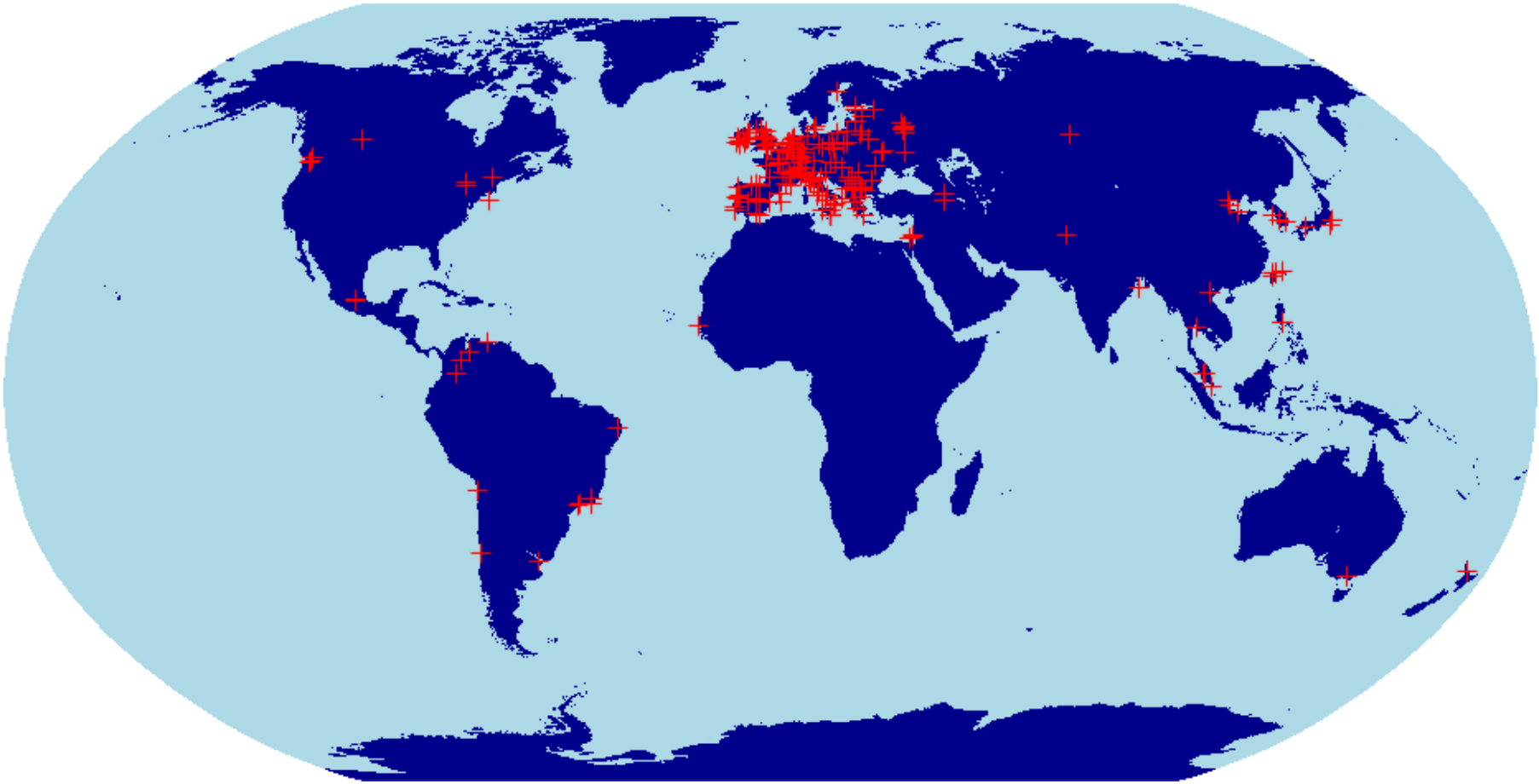
48h IR in 5min

Results, example areas to work on

- User traceability in pilot-job frame works
- Central emergency suspension service
- Forensic trainings

Incident Response in EGI

Incident Response in EGI



Incident Response in EGI

Impossible task:

- 54 different jurisdictions
- Sites are independent – very little centralized power
- Sites range from big national facilities to small underfunded departmental systems.
- Sites are usually already in the constituency of some other CSIRT.

How do you deal with this?

Incident Response in EGI

Impossible task:

- 54 different jurisdictions
- Sites are independent – very little centralized power
- Sites range from big national facilities to small underfunded departmental systems.
- Sites are usually already in the constituency of some other CSIRT.

How do you deal with this? You need to be:

- pragmatic
- humble
- and good at social engineering.

Incident Response in EGI

Basically, EGI is a federation of National Grid Infrastructures (NGIs) – typically one per country – that each encompass something between 1 and 40 physical sites.

Incident Response in EGI

- High level policies give a framework to operate in.
- Last resort – suspension. Follow the rules, or you can't be in our club.

Incident Response in EGI

- Each NGI has an appointed NGI security officer.
- A core subset (about a dozen) of the NGI security officers form the EGI Incident Response Task Force (IRTF).

Incident Response in EGI

IRTF members serve as EGI Security Officer on duty, on a weekly rota.

- Handle incident reports
- Keep an eye on monitoring
- Keep things falling between chairs

Incident Response in EGI

How to monitor the security status of the distributed sites?

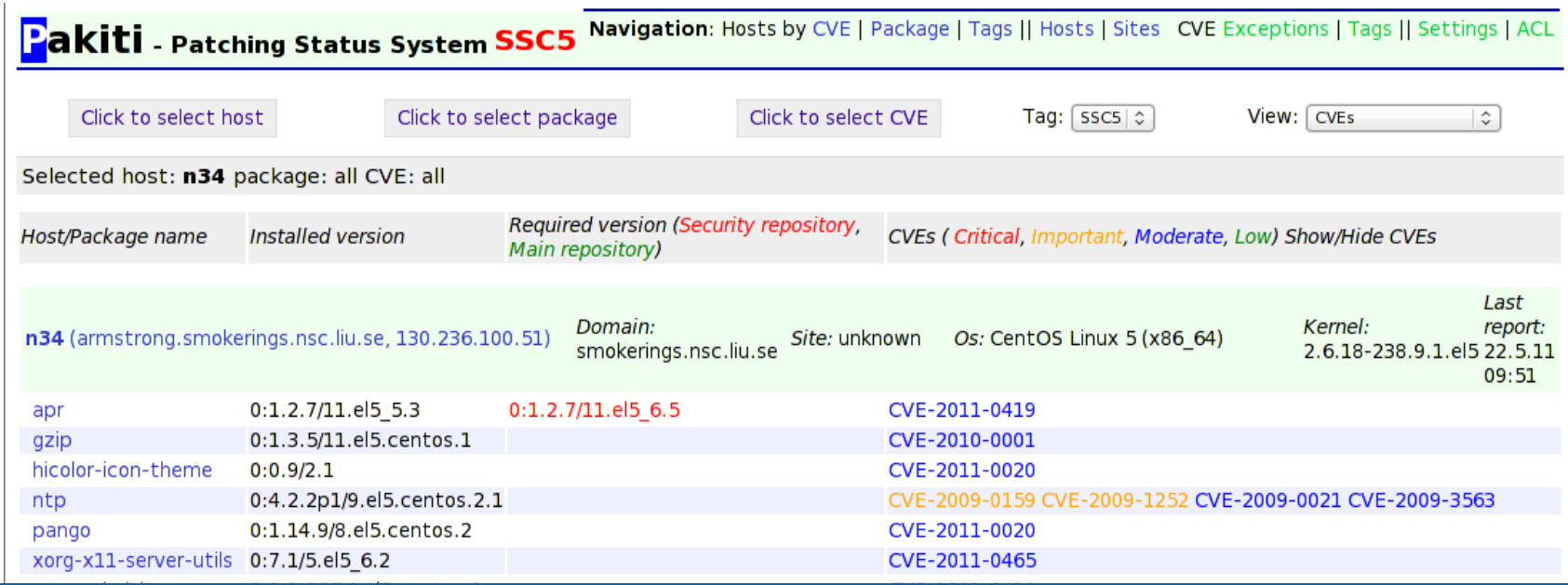
Realization: we have an infrastructure to run computation jobs!
Use that also for monitoring.

Nagios

- Monitoring jobs submit passive probe data into Nagios.
- Checks e.g. bad file permissions, vulnerable kernel modules.
- Used to quickly run custom tests across sites, e.g. to monitor CVE-2009-4033 which caused /var/log/acpid to be created with random permissions.

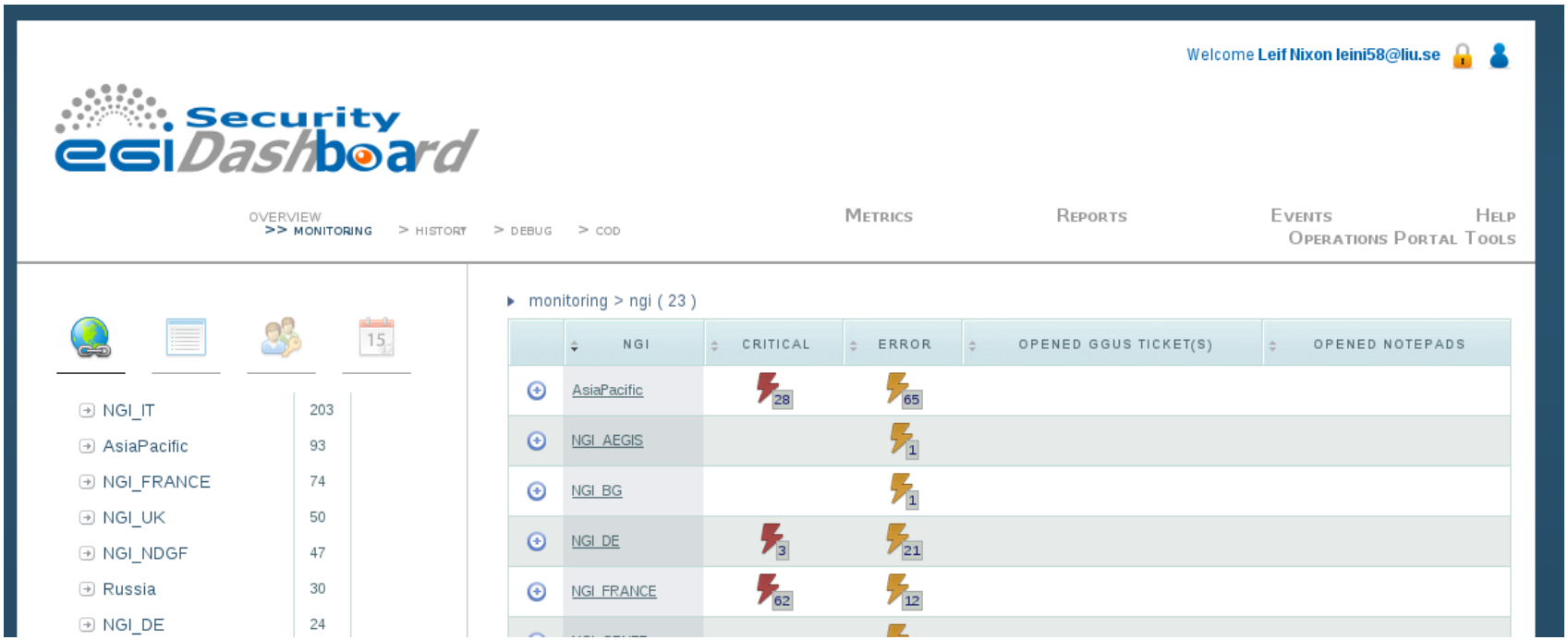
Pakiti

- Daily jobs dump the RPM data base and cross-checks against OVAL data.
- Web interface for monitoring, e-mail alerts for critical vulns.
- *Very* useful, but only gives results for a sample of the compute nodes at a site.



Security Dashboard

Monitoring data from Nagios and Pakiti are aggregated and presented in the Security Dashboard area of the Operations Portal.



Incident Response in EGI

- What happens when we get an incident?
- What *is* an incident?

Incident Response in EGI

- What happens when we get an incident?
- What *is* an incident?

An [grid] incident is any real or suspected event that poses a real or potential threat to the integrity of [grid] services, resources, infrastructure, or identities.

Anything can be labeled a grid security incident if you feel like it! (This is where you need to be pragmatic. . .)

Incident Response in EGI

The EGI incident response procedure is brief, but establishes a flat structure with maximum info sharing.

(This can sometimes conflict with some sites' non-disclosure policies, but if you have carefully established your trust relationships beforehand, we can usually get along.)

Incident Response in EGI

Each incident is assigned an IRTF member as incident coordinator, who

- issues a heads-up warning to all sites
- works with the victim site to investigate the incident, possibly issuing additional all-sites broadcasts as new information is discovered
- coordinates the incident with other players (VOs, CAs, other CSIRTs, law enforcement. . .)
- makes sure a closure report is sent to all sites

Incident Response in EGI

Total number of incidents involving grid technology:

Incident Response in EGI

Total number of incidents involving grid technology: 0

Incident Response in EGI

EGI-20110418-01	stolen ssh credentials
EGI-20110301-01	bruteforce ssh
EGI-20110121	web server misconfig
EGI-20111201-01	bruteforce ssh
EGI-20101018-01	bruteforce ssh
EGI-20100929-01	stolen ssh credentials
EGI-20100722	bruteforce ssh
EGI-20100707-01	stolen ssh credentials/remote vulns in CMSes
EGEE-20091204	stolen ssh credentials/X keyboard sniffing
GRID-SEC-001	stolen ssh credentials

Incident Response in EGI

- Large majority of incidents due to stolen or weak ssh credentials
- We have no power to force sites to deploy e.g. two factor auth
- We do try to motivate sites to install important security patches, partly to offset the potential damage from user level intrusions, and we also offer training for sysadmins (more on this later)

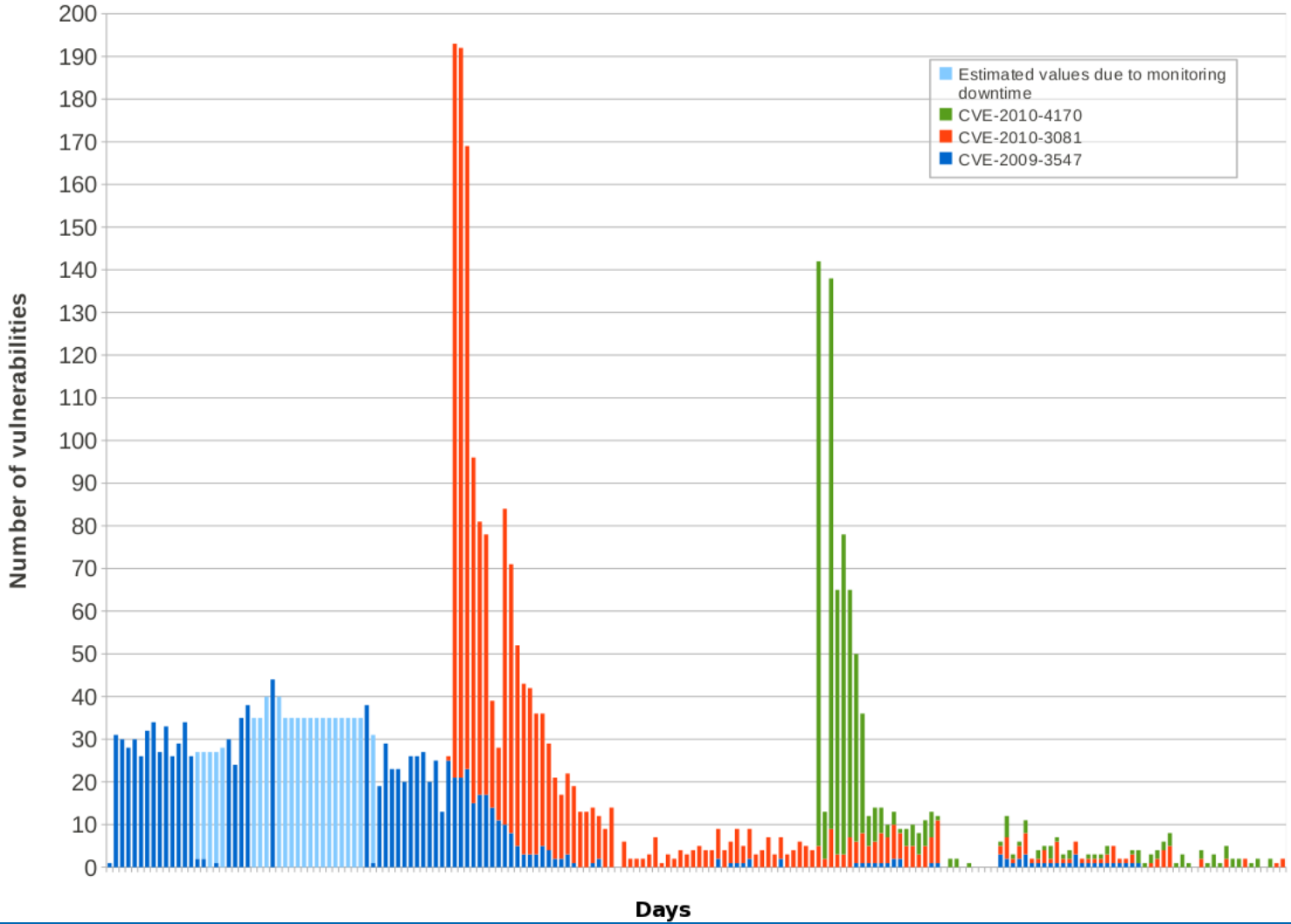
Incident Response in EGI

- Security Intelligence Group (SIG) monitors public and non-public sources for new vulns
- The Risk Assessment Team determines how serious new vulns are
- The EGI CSIRT produces detailed advisories that are broadcast to sites

Incident Response in EGI

- When new serious vulns appeared we used to issue an advisory, watch Pakiti for a while to make sure sites applied patches, and then forget about it.
- This didn't work; new vulnerable nodes keep appearing – bad config management, nodes that were under maintenance when patches were applied. . .
- We now continuously monitor for vulnerable nodes and slap them down as they appear.

Incident Response in EGI



Incident Response in EGI

A relatively new addition to our service portfolio is *security training for sysadmins*. (One training instance will be held here Tuesday–Thursday.)

In this course, the participants get full root access to a number of Linux systems, running more or less familiar services. The participants are divided into teams, and compete against each other.

Incident Response in EGI

The teams' task is to defend against and analyze realistic attacks of increasing sophistication, while keeping their systems up and running, and they are scored on their performance. This is challenging, exhausting and fun!

We also offer this course to other organizations – contact me if you are interested.

Incident Response in EGI

Finally, we try to be good community members and maintain good relations with neighbouring CSIRTs at all levels.

Any questions, comments, feel free to contact me.