

348 sites, 57 countries, 1 security team: Operational Security in EGI

Tobias Dussa, [tobias.dussa@kit.edu](mailto:tobias.dussa@kit.edu)

KIT <http://kit.edu> EGI-CSIRT <http://egi.eu>

Sven Gabriel, [sveng@nikhef.nl](mailto:sveng@nikhef.nl)

Nikhef <http://nikhef.nl> EGI-CSIRT <http://egi.eu>

Leif Nixon, [nixon@nsc.liu.se](mailto:nixon@nsc.liu.se)

NSC/SNIC/NDGF/EGI-CSIRT <http://egi.eu>



## EGI: European Grid Infrastructure

### EGI-CSIRT

#### Incident Response

#### 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

### NGI-CSIRT-View

### Thanks/Contact

- EGEE I- III 2004 – 2010
- Middleware Development
- Cluster management expertise at sites
- Operational procedures/policies

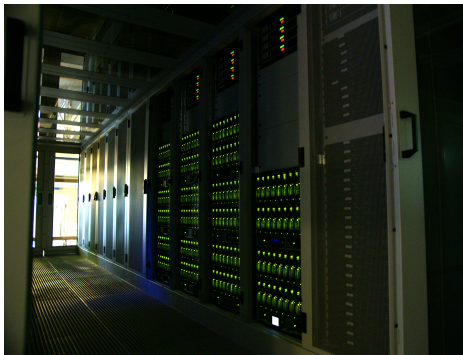


- EGEE I- III 2004 – 2010
- Middleware Development
- Cluster management expertise at sites
- Operational procedures/policies





- EGEE I- III 2004 – 2010
- Middleware Development
- Cluster management expertise at sites
- Operational procedures/policies

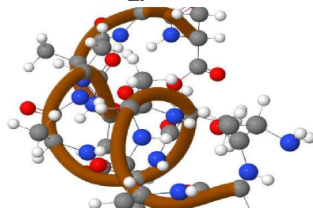
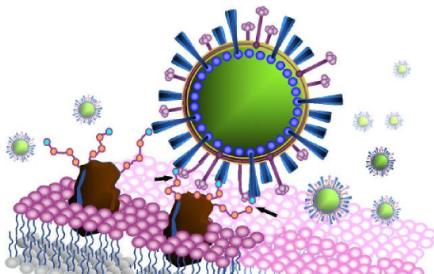
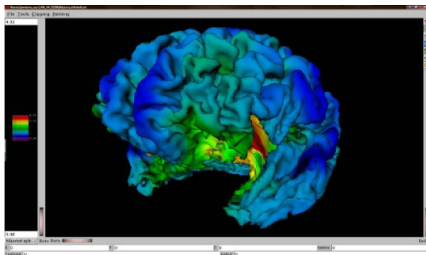


# EGI some numbers

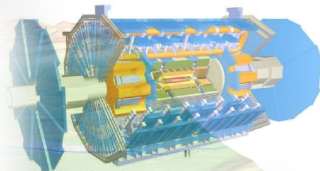




~ 12.000 Users globally  
~230.000 CPU-Cores  
200+ PB storage  
348 Sites globally  
10-40 Gbps network  
~28Million Jobs/Month



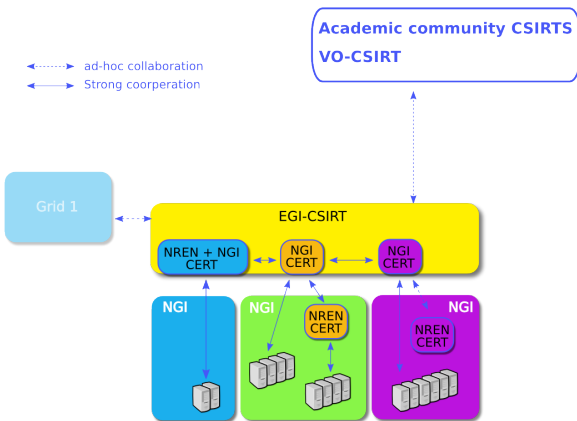
Atlas VO  
~3000 users  
~75000 cpu-cores  
~60 PB Grid-data Stored  
~10 PB/year Data rate  
100 + grid sites



Diameter: 26m  
Length: 50m  
Weight: 7000 t

Why does the universe look the way it does?  
What gives particles mass? The Higgs boson?

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



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

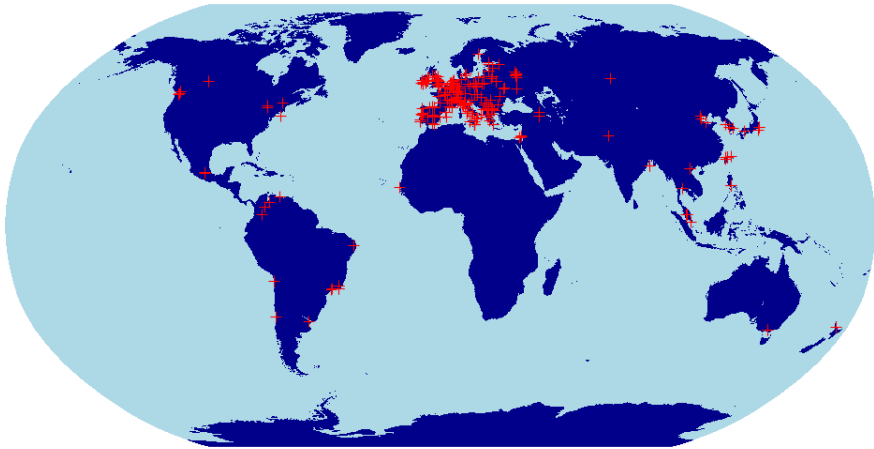
## EGI-CSIRT

Members: NGI-Security-Officers



## **Incident Response in EGI**





Impossible task:

- 58 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?

Impossible task:

- 58 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.

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

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

- 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).

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

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.*

**Pakiti - Patching Status System** **SSC5** Navigation: Hosts by CVE | Package | Tags || Hosts | Sites CVE Exceptions | Tags || Settings | ACL

Click to select host Click to select package Click to select CVE Tag: SSC5 View: CVEs

Selected host: **n34** package: all CVE: all

Host/Package name	Installed version	Required version (Security repository, Main repository)	CVEs (Critical, Important, Moderate, Low) Show/Hide CVEs
<b>n34</b> (armstrong.smokerings.nsc.liu.se, 130.236.100.51)	Domain: smokerings.nsc.liu.se Site: unknown Os: CentOS Linux 5 (x86_64)	Kernel: 2.6.18-238.9.1.el5 22.5.11 09:51	
apr	0:1.2.7/11.el5_5.3	0:1.2.7/11.el5_6.5	CVE-2011-0419
gzip	0:1.3.5/11.el5.centos.1		CVE-2010-0001
hicolor-icon-theme	0:0.9/2.1		CVE-2011-0020
ntp	0:4.2.2p1/9.el5.centos.2.1		CVE-2009-0159 CVE-2009-1252 CVE-2009-0021 CVE-2009-3563
pango	0:1.14.9/8.el5.centos.2		CVE-2011-0020
xorg-x11-server-utils	0:7.1/5.el5_6.2		CVE-2011-0465

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

- 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...)

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

(This is where social engineering comes in; it turns out professionally run CSIRTs have all sorts of privacy and disclosure policies that can hinder the information flow. You need to be able to bypass that in clever ways<sup>1</sup>.)

---

<sup>1</sup> Preferably without making lots of enemies

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

Total number of incidents involving grid technology:

Total number of incidents involving grid technology: 0

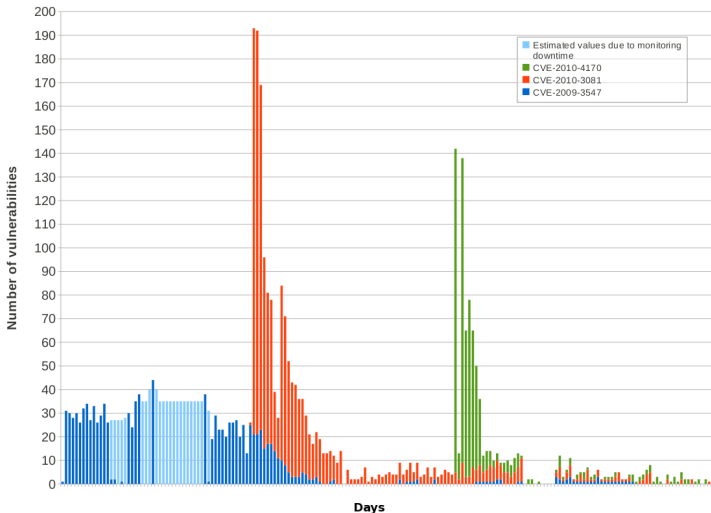


EGI-20110418-01	stolen ssh credentials
EGI-20110301-01	bruteforce ssh
EGI-20110121	web server misconfig
EGI-20111201-01	bruteforce ssh
EGI-20101018-01	bruteforce ssh
EGI-20100929-01	stolen ssh credentials
EGI-20100722	bruteforce ssh
EGI-20100707-01	stolen ssh credentials/remote vulns in CMSes
EGEE-20091204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

- 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

- 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

- 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.



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.

## **Security Drills**

**40 Sites, 20 countries, one global security exercise.**

Challenging our Incident Response Capabilities.

## Until now “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.



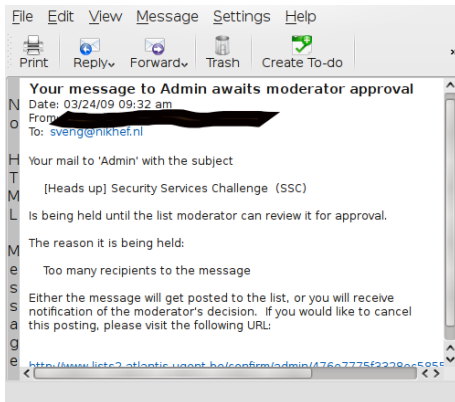
- **Communication:**

- 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.

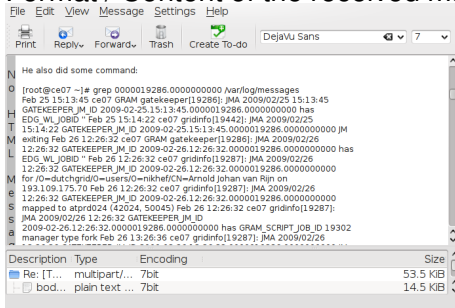
- **Communication:**

- Endpoints valid?
- Form/Content OK ?



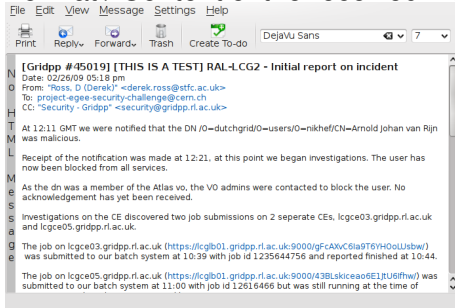
- **Communication:**
  - Endpoints valid?
  - Form/Content OK ?

## Format / Content of the received mails



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

## Format / Content of the received mails



- **Communication:**

- Endpoints valid?
- Form/Content OK ?

- **Containment**

- Ban "malicious" users
- Find/Stop malicious processes
- Find submission IP

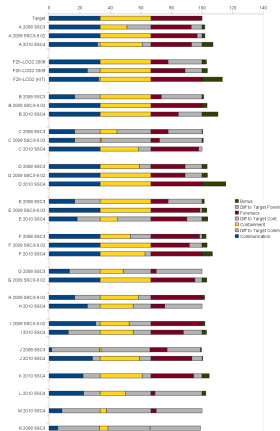
- Access Control

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

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



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



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

- Communication Templates

### EGI CSIRT: Incident reporting

EGI-CSIRT wiki

[Mission] | **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@egi.eu](mailto:abuse@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: egi@-
TO: egi-security-contact@milan.egi.eu;abuse@egi.eu
SUBJECT: Security incident suspected at «site» (CSG-IDB#): TLP: #NONE
**
** INFO: 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 for distribution restrictions **
Dear security contacts:
A suspected security incident has been detected at «site».
Summary of the information available so far:
«Info: A malicious SSH connection was detected from 012.012.012.012. The extent of the incident is
  
```



- 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**.*

- Communication Templates
- Generic Incidence Response Procedure
- Forensics guidelines

## Gather data

The data acquisition 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 filesystems/block devices 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 -auxwww > ps_auxwww.txt
netstat --program --netrim --verbose -n > netstat_pVn.txt
netstat --program --netrim --verbose > netstat_pVt.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_bIPnRSU.txt
for i in $(cat /etc/passwd); do lsof -a -s $(cat /etc/passwd | grep $i | cut -d: -f1) > lsof_a_${i}.txt; done
#-----
```

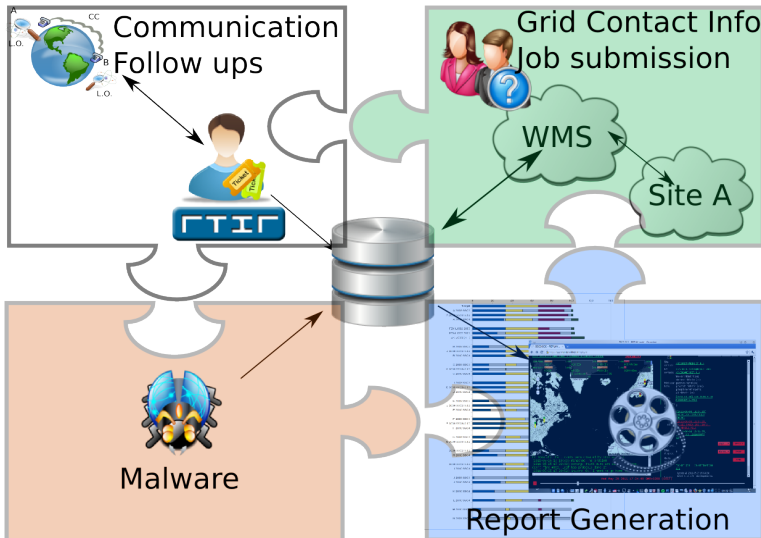
If there are suspicious processes that need further analysis, preserve the original binary and dump the program's memory:

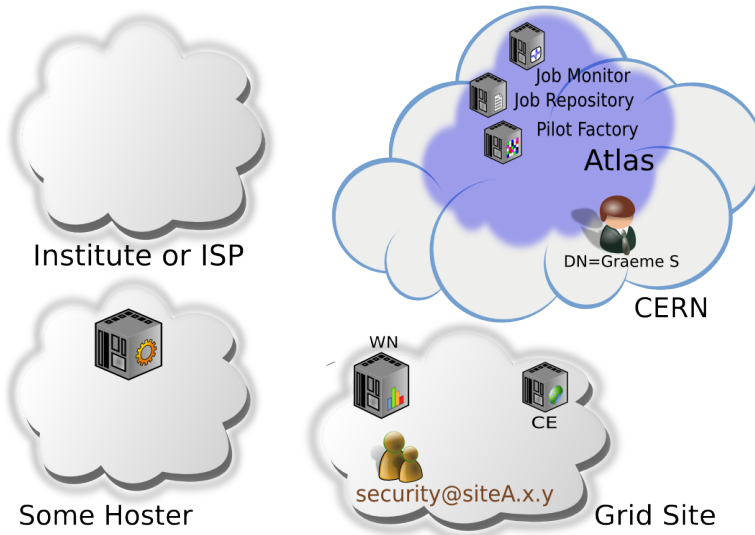
```
{ { {
#-----
export PID=12345 # <- INSERT PROCESS-ID (PID) HERE
kill -STOP $(PID) # stop process
cp /proc/$(PID)/exe $(PID).exe
# some distributions have a script called 'gcore' which does this in batch-mode
gdb -p $(PID)
# type 'gcore', then 'detach' and 'quit'
# The program's memory is now saved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

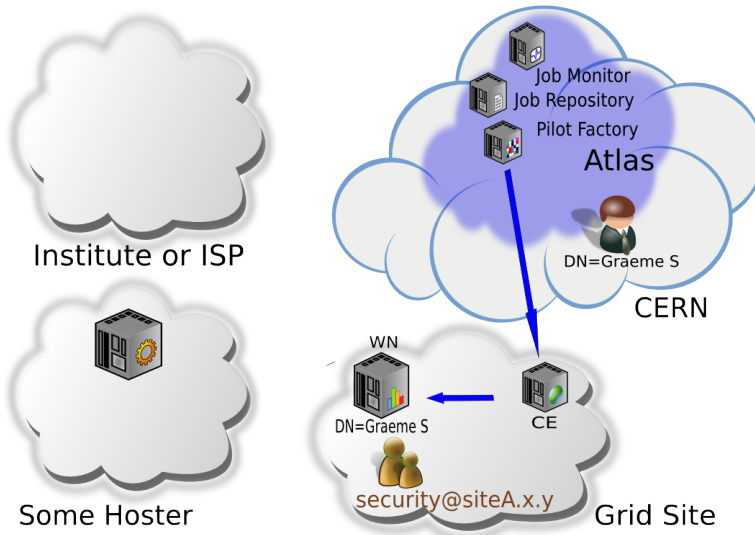
## **Security Drill Framework allows for:**

- 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.

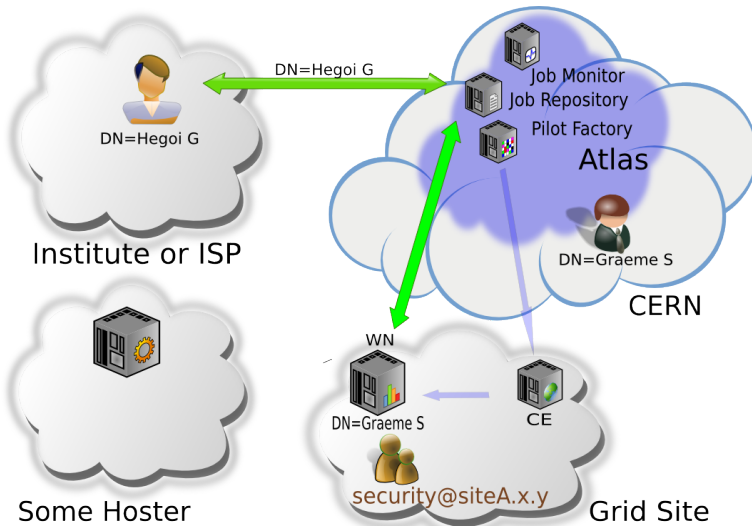
- Per site training exercise.
  - “You are on your own”, limited external information source
  - Training Site-operations, goal: improve/measure site response capabilities, procedures.
- Multi site incident simulation exercise.
  - Various information sources / focus on collaboration/information sharing





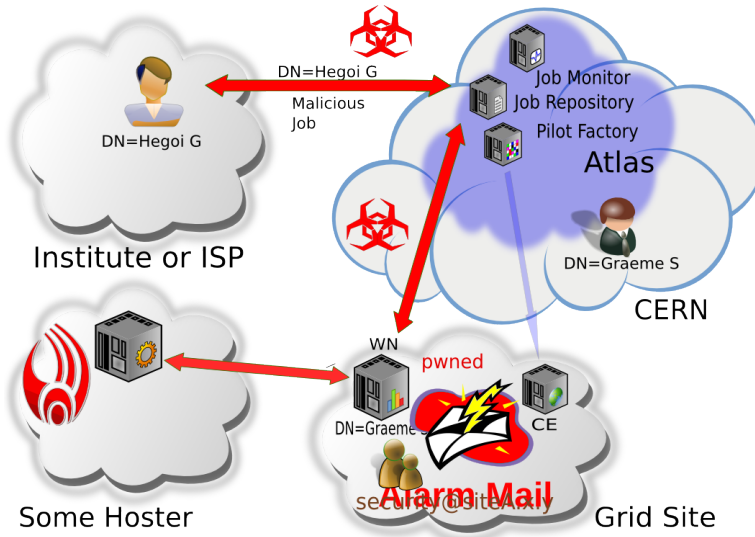


# SSC4/5 Scenario





# SSC4/5 Scenario



## Introduction to the Security Exercises Framework

## Layout:

- Realistic Simulation of an Incident involving CSIRTS at 40 sites in 20 countries and a VO
- Malware (Bot-Net) was deployed with help of a VO-Job-Submission Framework
- Alerts have been sent out to 2 affected sites

## Targets/Expected Results:

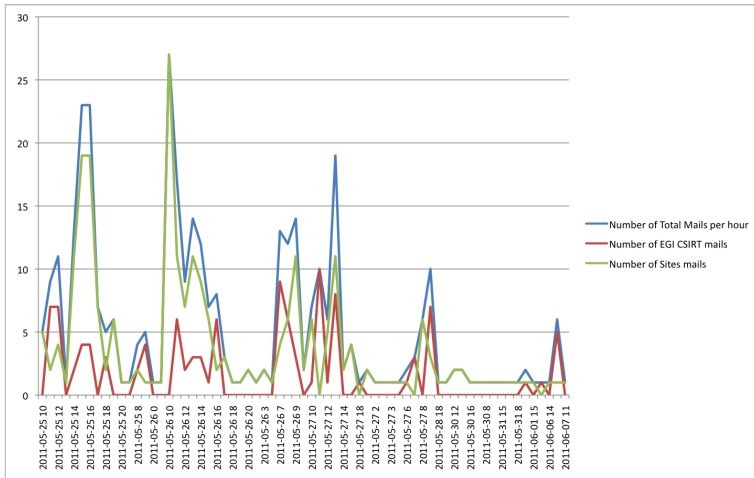
- Project wide incident response capabilities.
- Trigger ad hoc Collaboration (EGI-CSIRT, VO-CSIRTS, CAs, ...).
- How long does it take to get the incident contained?
- Efficiency of security operations?
- Effects on the resource availability?
- Operational Problems in Incident Handling?
- Identify Experts: Forensics, Network-Analysis
- Assessment of tools used

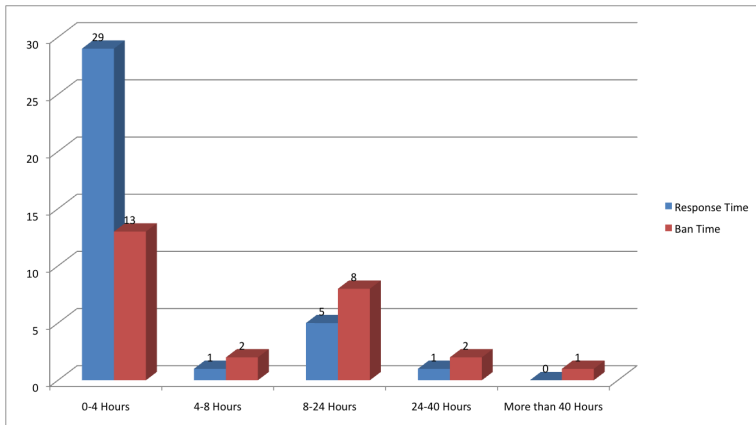
## 48h IR in 5 Minutes

## Early results:

- Operational: Targeted response difficult.
- Containment had a serious impact on the availability.
- Access management at some sites not sufficient.
- High communication load on incident coordinators

# SSC-5 Preliminary Results







## **A Site CSIRTS View**

This part provides a site's view of a security service challenge. It tackles the following questions:

- Why forensic analysis?
- Where and how to gather evidence?
- How to analyze evidence data?
- What does it feel like to be challenged by an SSC?

It does *not* address:

- How to contain damage?
- What to communicate when to whom?
- How to recover from an incident?

To assess and answer several important questions about the incident:

- Where did the attacker come from?
- How was access gained?
- What damage was done?
- What other machines were affected?
- ... and many more related questions.

- Broad classes of data sources:
  1. Highly volatile (e. g., CPU registers),
  2. Volatile (e. g., RAM),
  3. Static (e. g., hard drives), and
  4. Highly static (e. g., archive tapes).
- More volatile evidence must be gathered and preserved first, if possible.
- Obviously, not all classes available or applicable in every instance.

Usually, this is the first thing to do.

1. Collect all relevant network-related data:

- NAT data,
- proxy data,
- netflow data,
- and so on.

No problem if there are log files, interesting if not (live NAT tables etc.).

2. Correlate data to find your suspect host, if any.

. . . or at least a suspect machine. Now what to do?

1. Gather general information and evidence:

- Running processes,
- open network connections,
- who is logged on,
- who was logged on,
- mounted devices
- and their mountpoints,
- etc.

2. Look if there is anything suspect.

What to do with your suspect (process):

1. Stop the process (do *not* terminate it!).
2. Collect and secure:
  - the binary being executed,
  - its core memory,
  - its shared memory regions, if any,
  - its file handles,
  - other volatile data.

Finally, collect less volatile stuff:

- If possible and sensible, power off the machine and grab the hard drive.
- If not possible or sensible, at the very least collect the following stuff:
  - All related log files,
  - any files involved in the incident,
  - actually, if possible, the entire file system.



Take a close look at the collected data. Some pointers:

- Inspect suspect executables (with `strings`, `hexdump`, `gdb`, `rec`, `IDAPro`, ...).
- Look at core dumps (using `gdb`).
- Grep through log files and the like.
- Check files' MD5 sums against the known-good list.
- Perform further filesystem analysis, for instance with `autopsy` or `rkhunter`.
- If necessary, iterate.

- Information provided in the alert mail:
  - IP addresses 192.108.46.248 and 195.140.243.2 are evil.
  - (End of list!)
- Unknown: Everything else, particularly:
  - Are the bad IPs involved with our systems?
  - If so, how?
  - And what happened, if anything?

- First step: Find out whether the IPs in question have shown up at our site.
- Problem: All grid resources are behind a NAT.
- Sifting through the appropriate logs yields a machine connected with the suspect IPs (boring).
- Surprisingly, we have a winner!
- (Watch out for timestamp time zone!)

Culprit process was quickly identified (no stealth measures).

- Job was submitted via Panda.
- Panda logs show
  - what DN was used to submit the actual job and
  - what host the actual job was submitted from.
- Next step, obviously: Dump all the information we can get.

- Running the binary through `strings` reveals some fishy strings in the binary:  
JOIN, NICK, PONG, PRIVMSG, USER
- Disassembling yields information about:
  - Communication and
  - other activity.
- Inspecting the core dump gives actual ID strings used in communication.

After reverse-engineering, this was known:

- Binary was an IRC bot (communication endpoints and parameters known),
- (tried to) install
  - at job and
  - cron jobto become persistent, and
- (tried to) transfer `/etc/passwd` out to drop site, but
- no root exploit used and no root kit installed.

Things to watch out for when doing forensics:

- Modifying evidence while collecting (e. g., file access times).
- Dropping volatile evidence (e. g., memory content).
- Failing to document actions properly (timestamps!).
- **IMPORTANT:** If the incident looks like it will involve legal action, **stop everything you are doing** and **call the police!**

Common sense and good practices:

- Prepare a checklist.
- Strictly separate evidence acquisition and evaluation.
- Gather evidence, then produce a working copy of the evidence locker, then work on the working copy only.
- Go out of your way to ensure you work in read-only mode whenever possible, even on the working copy.
- And, most importantly, if you are unsure what to do, talk to somebody who has a better chance of knowing.



## **Security-Exercises Monitor (Contact: [ssc@nikhef.nl](mailto:ssc@nikhef.nl))**

- Aram Verstegen (Nikhef, <http://www.nikhef.nl>)
- Oscar Koeroo (Nikhef, <http://www.nikhef.nl>)
- Sven Gabriel (Nikhef, <http://www.nikhef.nl>)
- Carlos Fuentes Bermejo (RedIRIS, <http://www.rediris.es>)
- Movies are available from: [Introduction to the Security Exercises Framework, 48h IR in 5 Minutes](#)

## **SSC-5**

- Graeme Stewart / ATLAS-CSIRT (ATLAS, <http://atlas.ch>)
- EGI-CSIRT (<http://www.egi.eu>)
- Participating NGI-CSIRTs and Site-CSIRTs