SSC-5, 40 Sites, 20 countries,

challenging our Incident Response Capabilities

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

Introduction

- Earlier SSCs
- SSC5 goals, Preparations, Participating sites
- Security Drills infrastructure
- SSC-5 Security Incident involving a VO-Job-Submission Framework

Summary

Thanks/Contact

Objective SSC-1 – SSC-4

http://osct.web.cern.ch/osct/ssc.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.

Objective SSC-1 – SSC-4

- SSC1: Trace a job (WN $\rightarrow$ CE $\rightarrow$ RB $\rightarrow$ UI).
  - Basic capabilities, can the site-admins trace a user job?
- SSC2: Trace storage operations (file create, move, delete,...).
  - Storage did not provide sufficient logging to solve the challenge, tested savannah as a communication method.
- SSC3: Realistic simulation of a security incident. “Consider any activity from the following user as malicious. DN: ....”.
  - Incident-Response tasks: Communication, Containment, Forensics got evaluated.

Objective SSC-1 – SSC-4

- SSC3-9.02: SSC3 re-run. Replaced RB with WMS.
  - OSCT provided sites with supporting material as: Communication Templates, Incident Response Procedure.
  - SSC3-9.02 Was also run in most of the regions, challenging approx. 133 Sites
- SSC-4
  - IPs used as starting point for the investigations in SSC4
  - Atlas Job-Submission framework, 2 certificates involved
  - New malware (bot net)

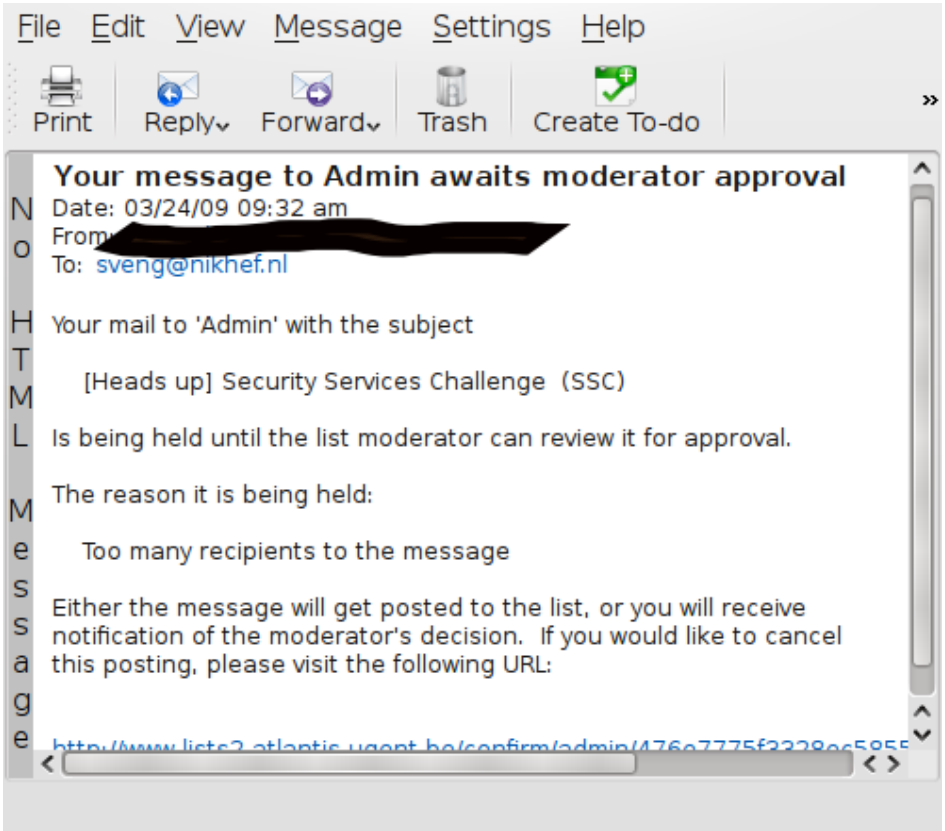
Security Drills / Results

- 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- Problems: Drill-Alarm ignored, contact address wrong, outdated, ...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

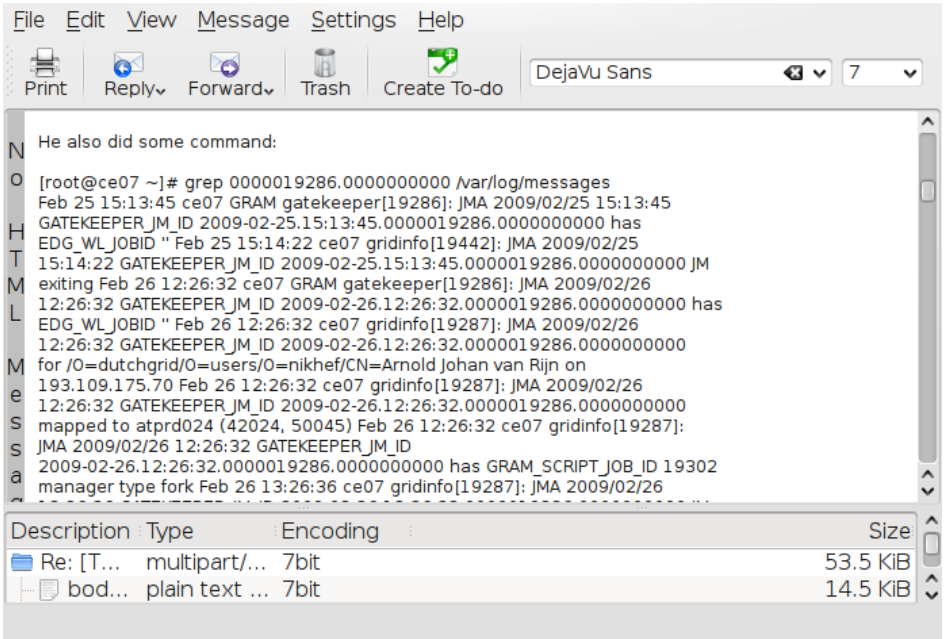
- Communication:
  - Endpoints valid?
  - Form/Content OK ?



Security Drills / Results

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

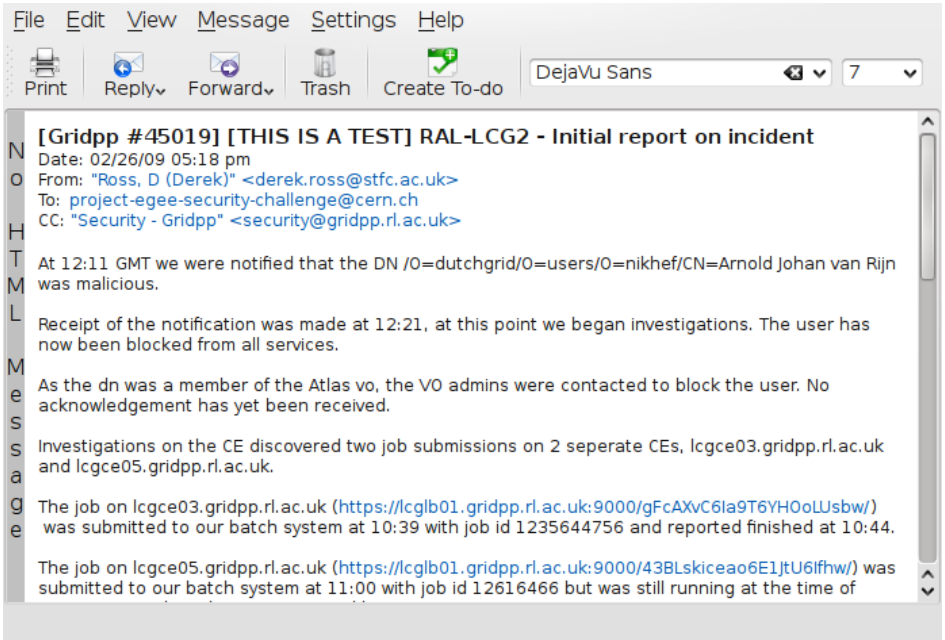
Format / Content of the received mails



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

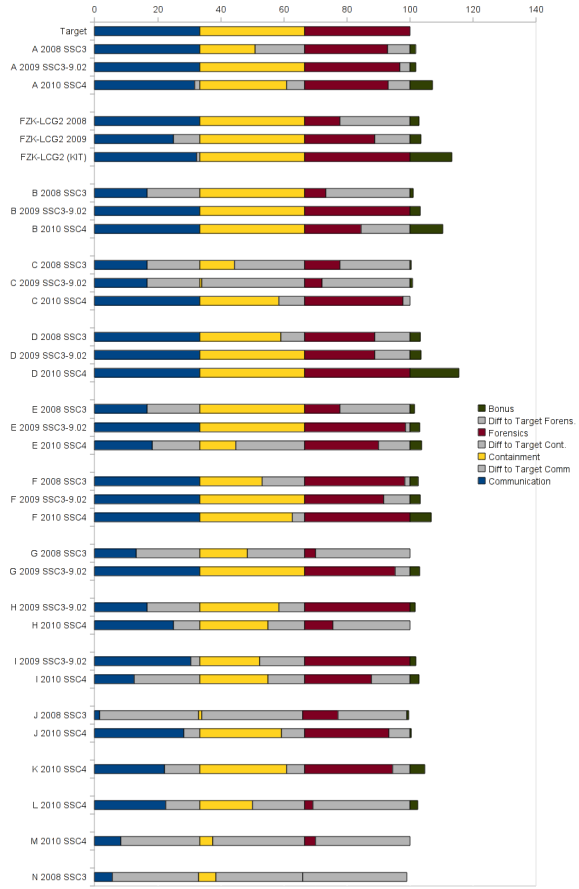
- Access Control
- X.509 based Authentication
- Definitive access control at the sites. (DN in Textfiles), ... really?
- User-certificate information gets mapped to a unix account

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



Earlier Run Results

	Reaction time in *h*		User Management	
Exercise	Heads-Up	Stop Procs	Success %	Time needed
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)

- Pilot-Job-Submitter (PJU), Pilot-Job-User (PJU)
- PJS banning based on Panda logs
- 25% did not ban the PJU at all services

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.

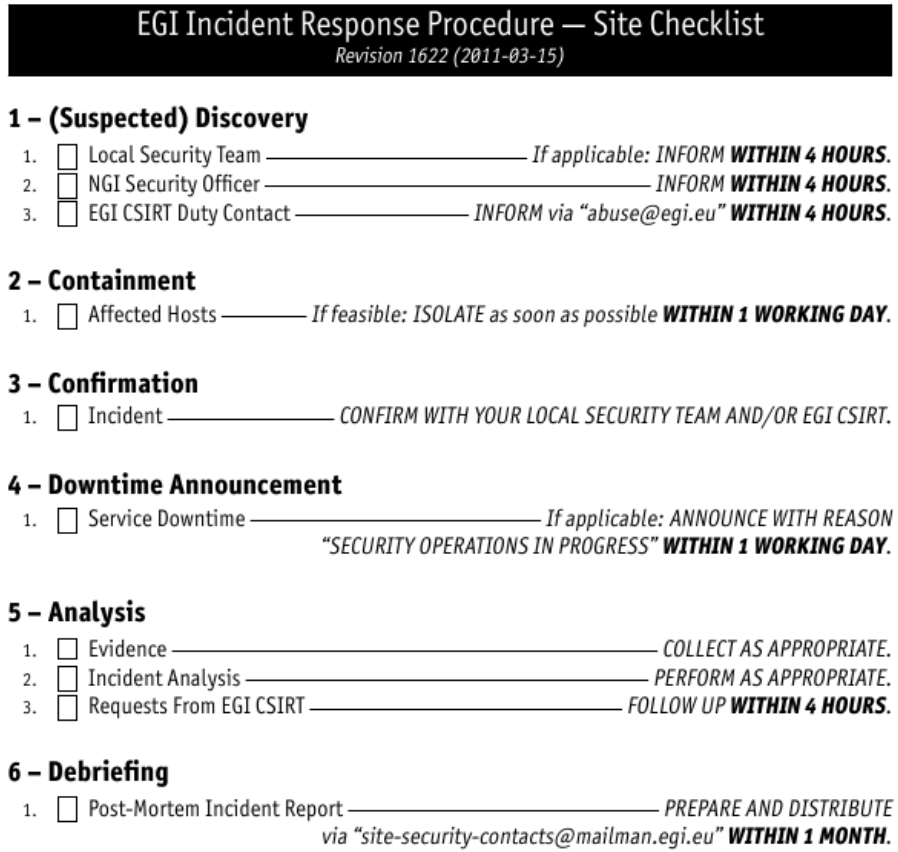
Initial HEADS-UP message [edit]

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

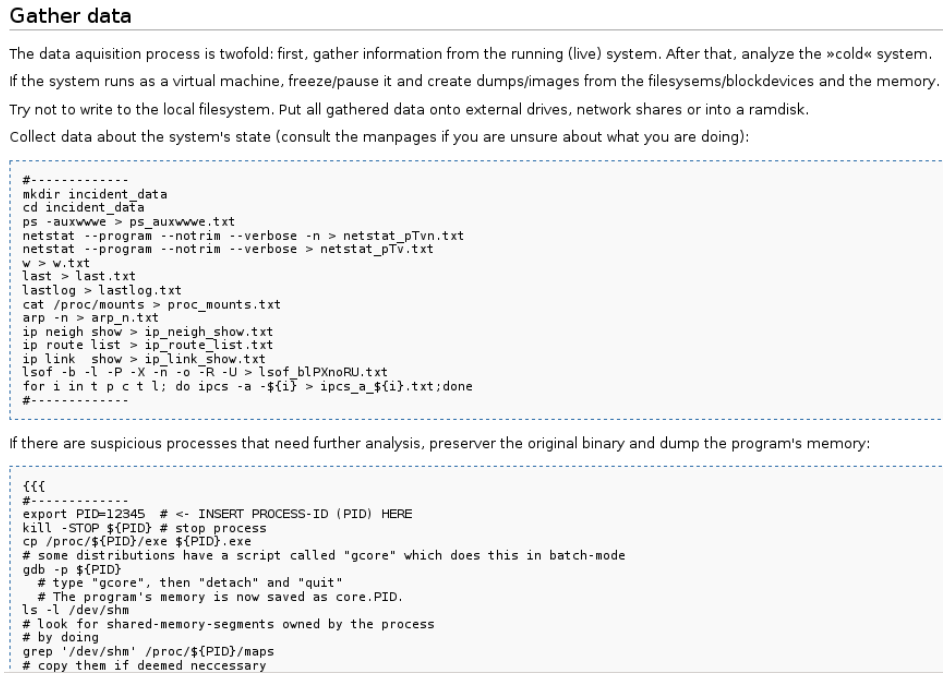
1. ☐ Evidence — *COLLECT AS APPROPRIATE.*
2. ☐ Incident Analysis — *PERFORM AS APPROPRIATE.*
3. ☐ Requests From EGI CSIRT — *FOLLOW UP* ***WITHIN 4 HOURS.***

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
```

Sites got Supporting Material

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.

SSC-Monitor Framework

- Per site training exercise. (Under Development)
  - To be initialized by the sites
  - “You are on your own”, limited external information source
  - Training Site-operations, goal: improve/measure site response capabilities, procedures.
  - Evaluation via a web form.
- Multi site incident simulation exercise. (used in SSC-5)
  - Various information sources / focus on collaboration/information sharing

SSC-Monitor Framework

Security Drill Framework allows for:

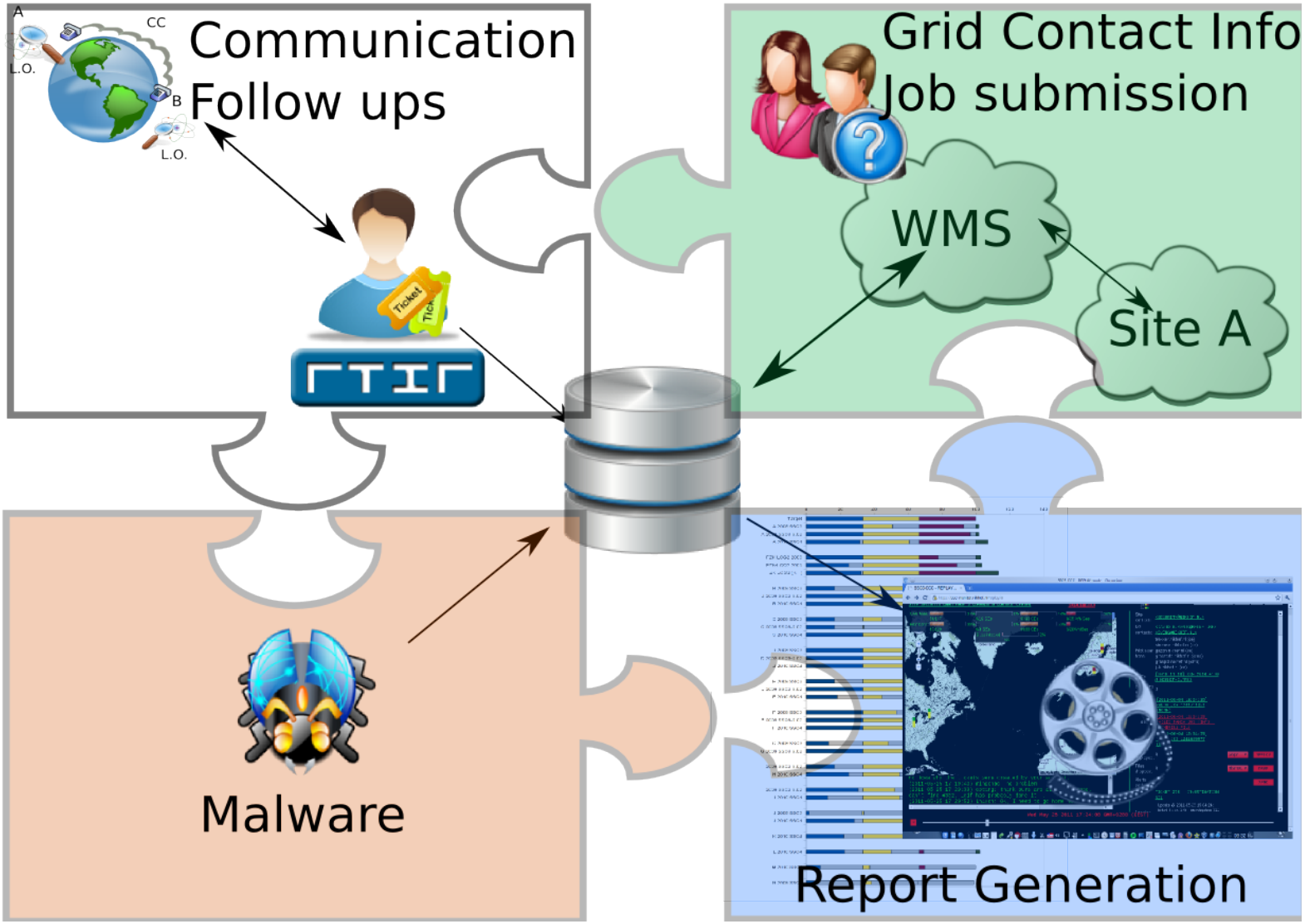
- Various job-submission methods, Storage operations.
- Define set of tasks (Communication, User/Process management with target times)
- ”Automated” Report generation / Scoring schema.
- Keep history/monitor Progress.

SSC-Monitor Framework

Evaluation:

- Automated analysing the database content.
- Evaluation per Task/Site/NGI possible.
- Status of the sites progress/status can be viewed during the run.
- SSC can be ”replayed” on the map

SSC-Monitor Components



SSC-Monitor Components

Modules

- Database (Site-Location, Job-activity, Environment, User-management, Storage-System, Ticket-Status, Sites-Operations)
- Map:Database information will be displayed on googlemaps
- Provide interfaces to Job submission glite/panda and Ticket Creation.
- Communication/Ticketing System, Communication-Templates.
- Pakiti (what is the CVE situation on the host where the SSC is running)

SSC–Monitor Intro

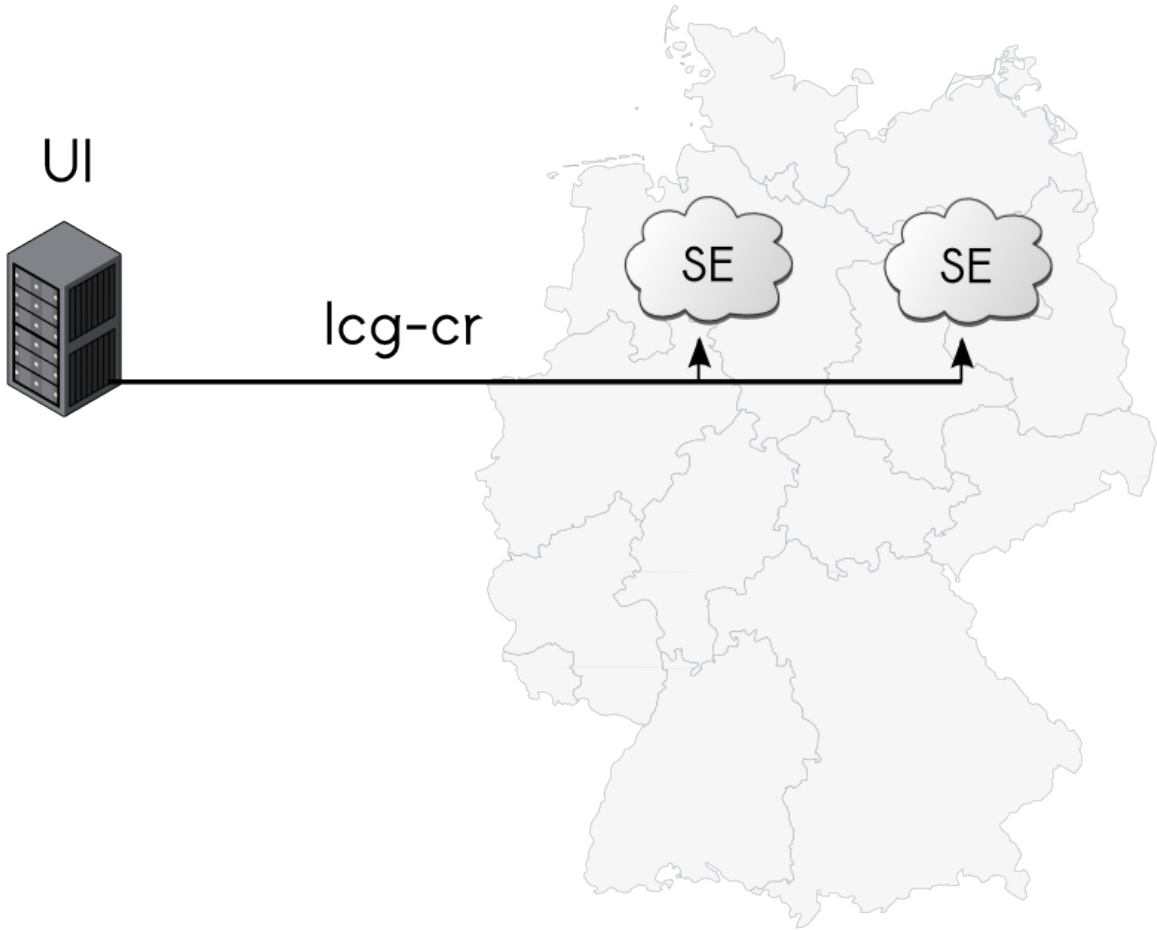
SSC-5 Preparation/Layout

- Negotiate with VO (Thanks Atlas), Find attacker ID (Thanks Hegoi)
- EGI-CSIRT F2F April 6th 2011
  - Run Details
  - Identify Sites, NGIs were asked to suggest sites to participate (max 4)
    - UK was very cooperative and participated despite of a sites evaluation
    - IL did not provide sites
    -
  - Introduction to RT-IR (Carlos Fuentes)

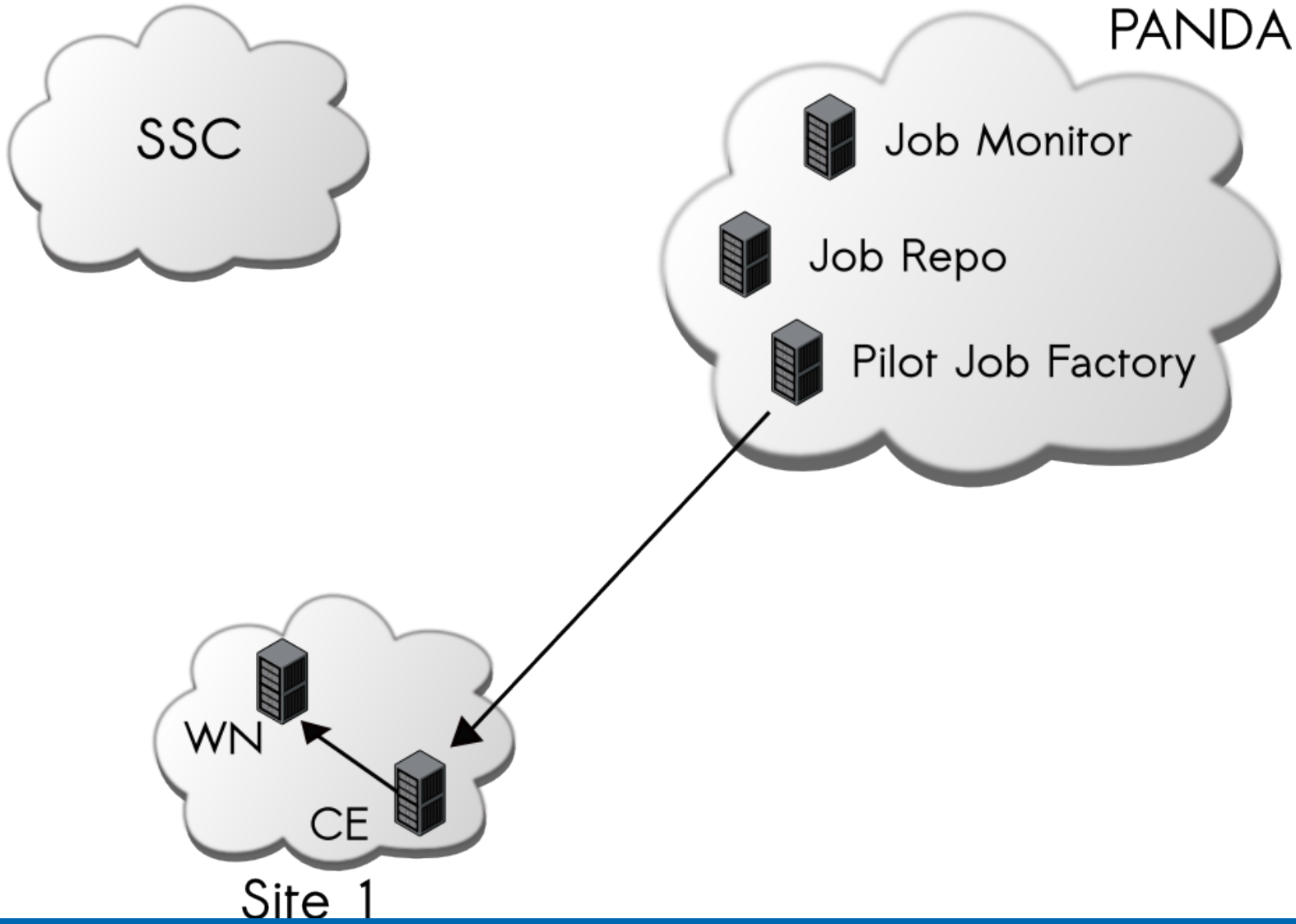
SSC-5 Preparation/Layout

- Announcements, additional info sent to the sites.
- Done with Communication templates in RT-IR
- 1 Week before start: Check validity of contact details, Announce the SSC-5, ask for confirmation.

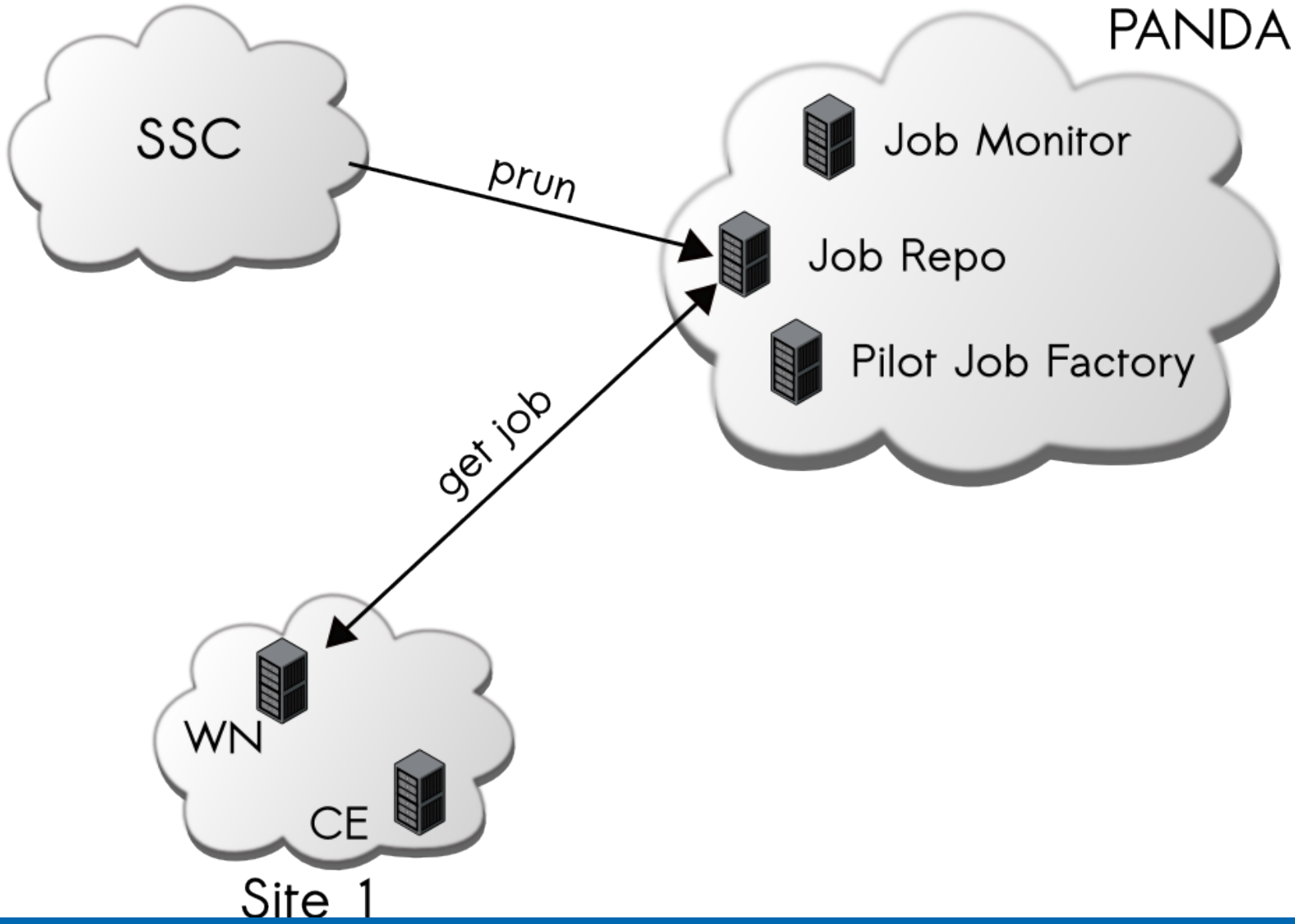
SSC-5 Preparation/Layout



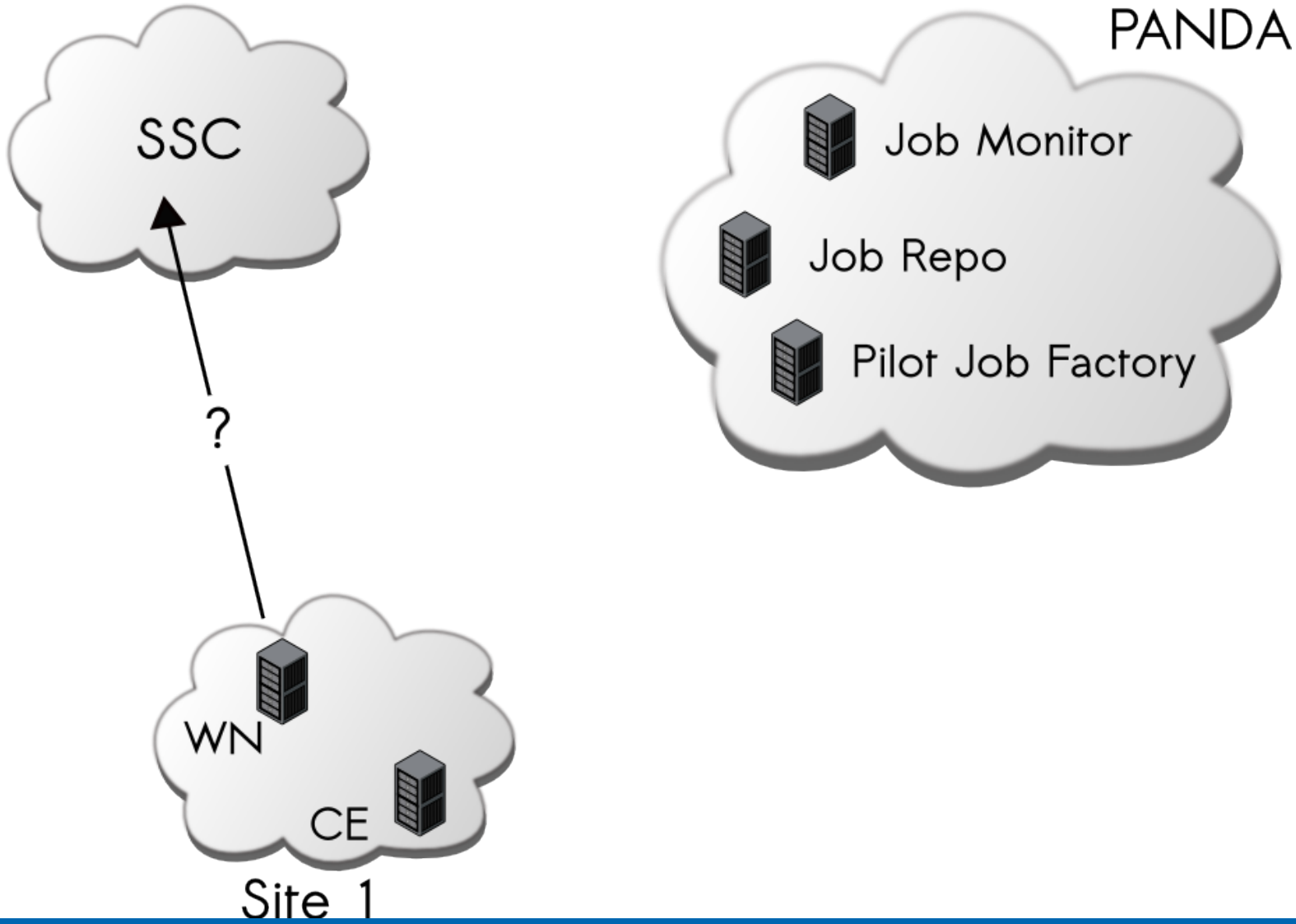
SSC-5 Preparation/Layout



SSC-5 Preparation/Layout



SSC-5 Preparation/Layout



SSC-5 Layout / Targets

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

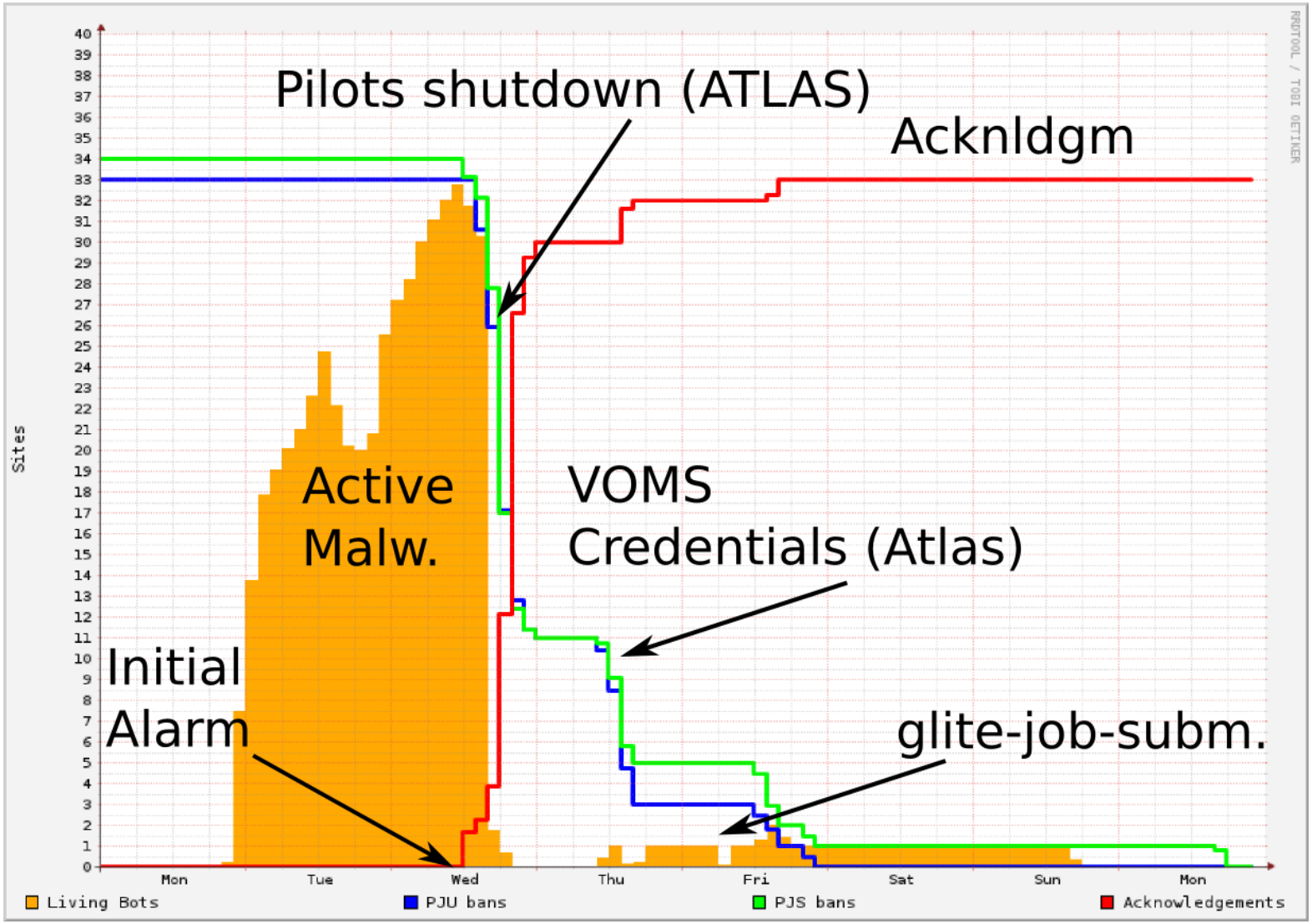
SSC-5 Layout / Targets

Targets/Expected Results:

- Project wide incident response capabilities.
- 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
- Trigger ad hoc Collaboration (EGI-CSIRT, VO-CSIRTS, CAs, ...)

48h IR in 5min

SSC-5 Preliminary Results



SSC-5 Preliminary Results

- Storage Element: 30% of the sites found the file copied earlier to the SE
- Operational: Targeted response difficult for the sites.
- Containment Job/Process Management: serious impact on the production
- Access management at some sites not sufficient
- User-Management in Pilot-Job-Framework: Fine grained access control not possible at the sites
- High communication load on incident coordinators

SSC-5 Preliminary Results

- Strong collaboration between VO/Site/NGI/EGI CSIRTS is crucial (was rated as very good)
- Experienced Sites/Teams provide useful information/tools (Network/Binary Forensics)
- Fabric Management Systems used at most sites, not used for Access-Management
- Log-Analysis: locally developed tools, sites rely on external information source (Panda)
- Time spend on the incident:4 - 40h, 3 sites 16h +, most sites less 8h

SSC-5 Preliminary Results

- RT-IR: Automation of work-flows, Templates
- Coordinated Communication between Teams to minimize mail traffic
- Instant Messaging: Found Usefull by all NGIs

SSC-5 Preliminary Results

- Comments/Concerns raised by the sites:
- Privacy issue of the panda service
- Traceability of user activity at the sites relies on 3rd party logs
- User/Access management

Thanks

Security-Exercises Monitor (Contact: 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