SSC Framework – SSC-5

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

SSCs Motivation/Purpose

- SSC-1 – SSC-4

SSC Framework

- Design / Components

SSC-5

- SSC-5 Layout / Participating Sites
- Status
- ToDo
- Expected Results
- SSC5 – what to address

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 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.

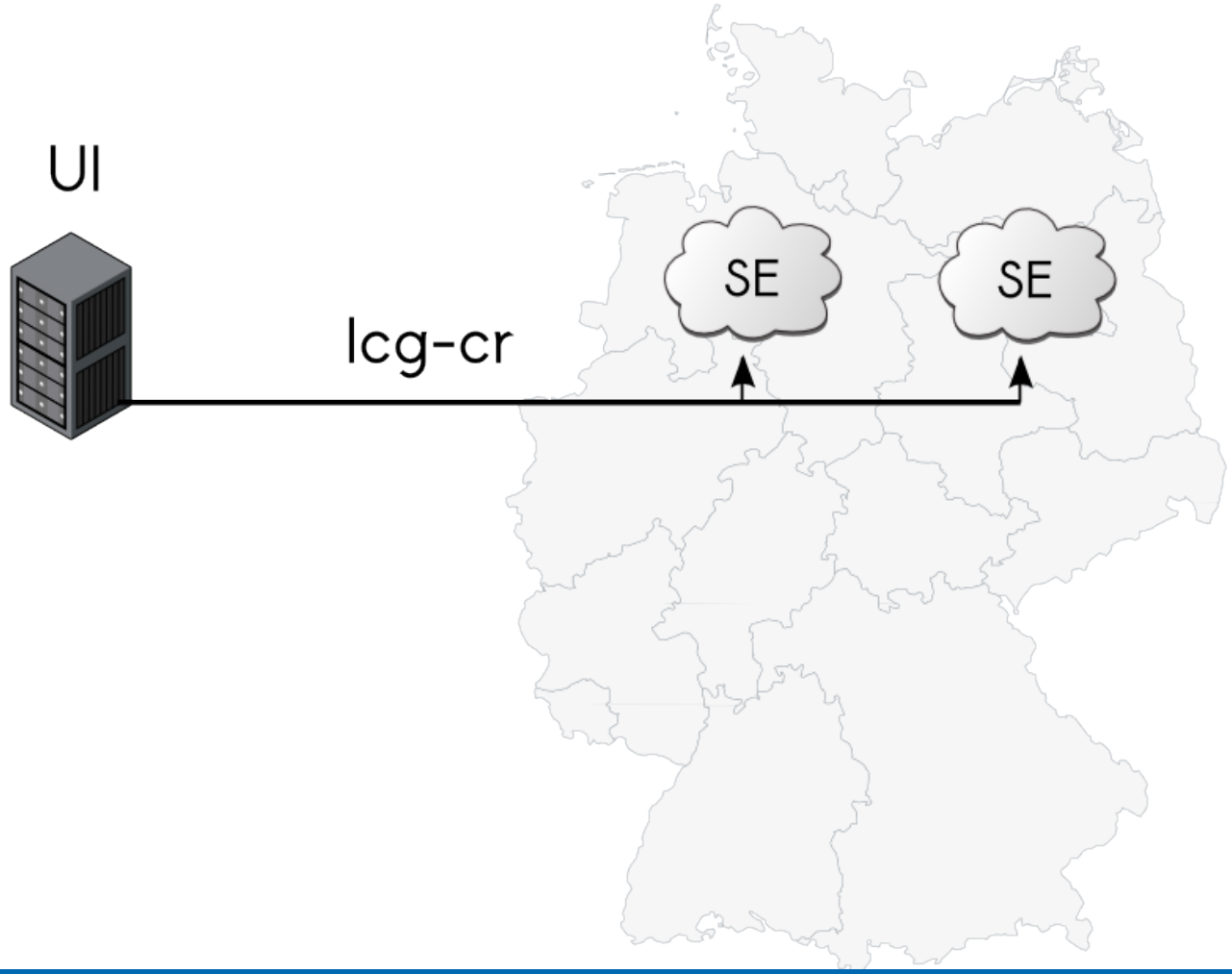
Objective SSC-1 – SSC-4

- SSC3-9.02: SSC3 rerun. Replaced RB with WMS.
  - OSCT provided sites with Communication Templates,Incident Response Procedure.
  - Regional Runs (ca. 133 Sites)
- SSC-4
  - Starting point IPs
  - New malware (bot net), interesting Feedback KA/Eygene!
  - Atlas Job-Submission framework, 2 certificates involved
  - Sites have Problems to operate on 2 Certificates properly
  - New Site (ARC, JSI, Slovenia did quit bad. No Response Plan/Procedure?
- All these challenges Attacker/Coordinator/Evaluator in one Person, I found this always difficult.

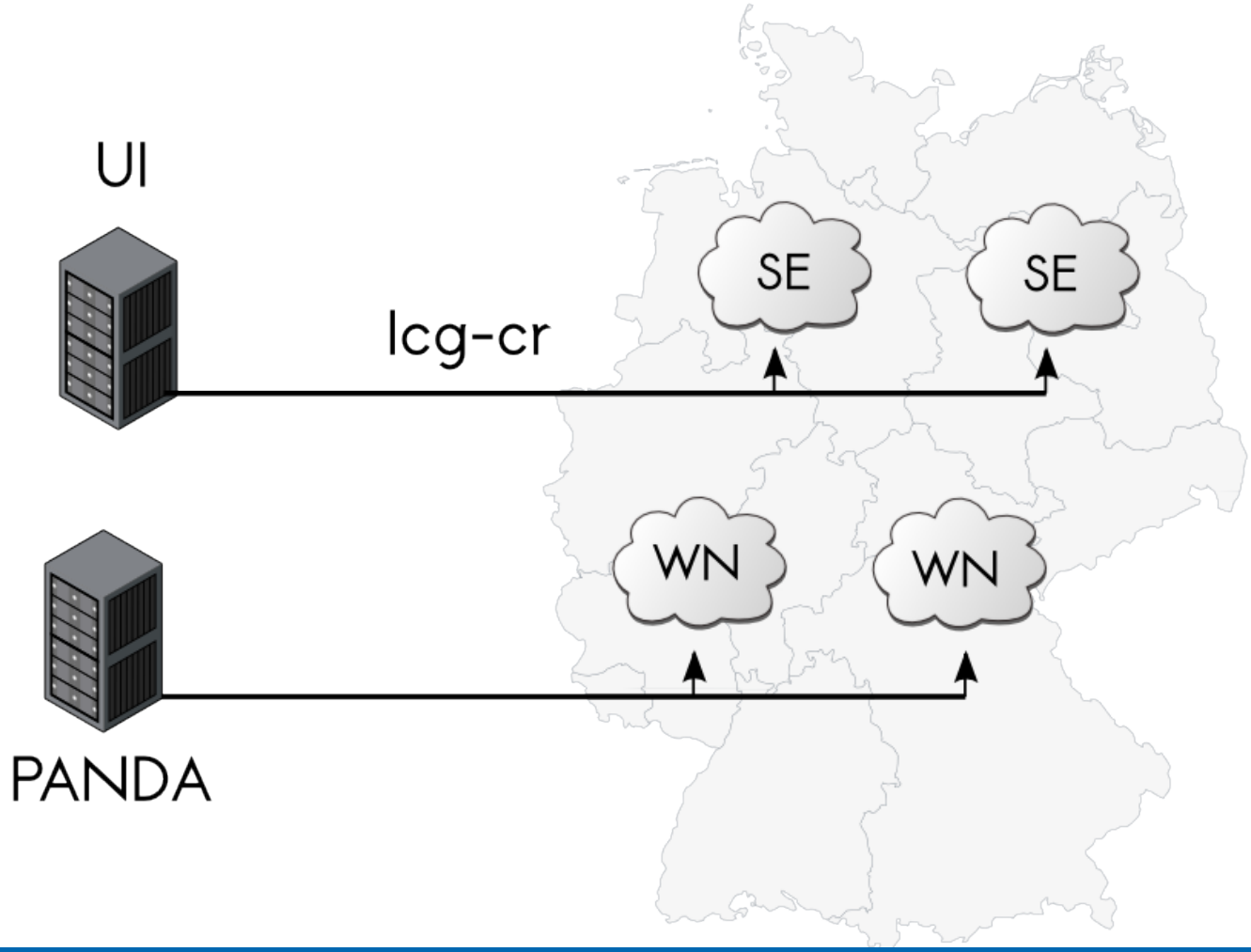
Evaluation SSC-1 – SSC4

- Based on excel sheet.
- Scoring based on time stamps.
- Manually evaluating mails, tedious, human factor, results not easy to compare.
- Should be improved, see discussion at the end of the talk

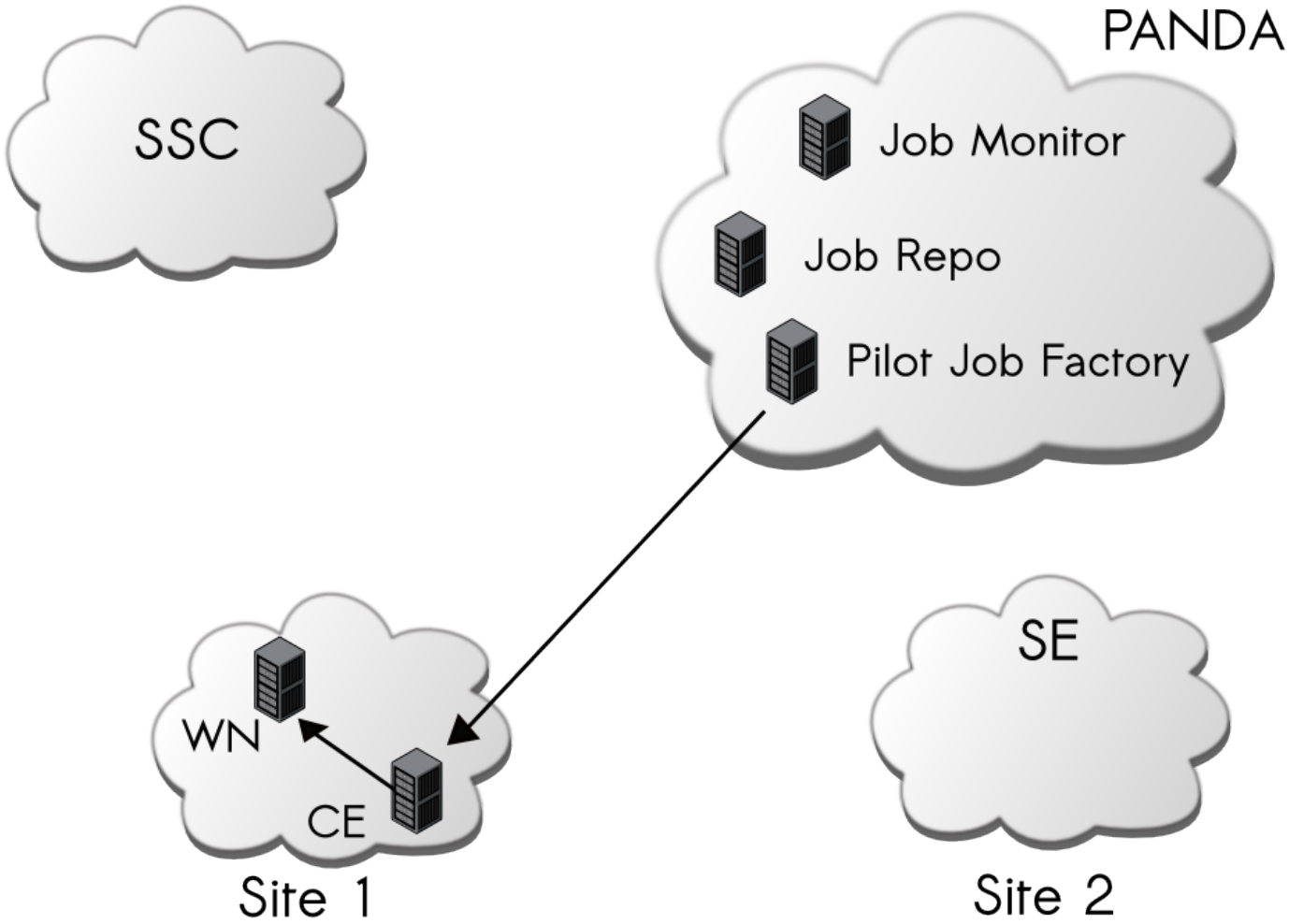
SSC-5 Layout



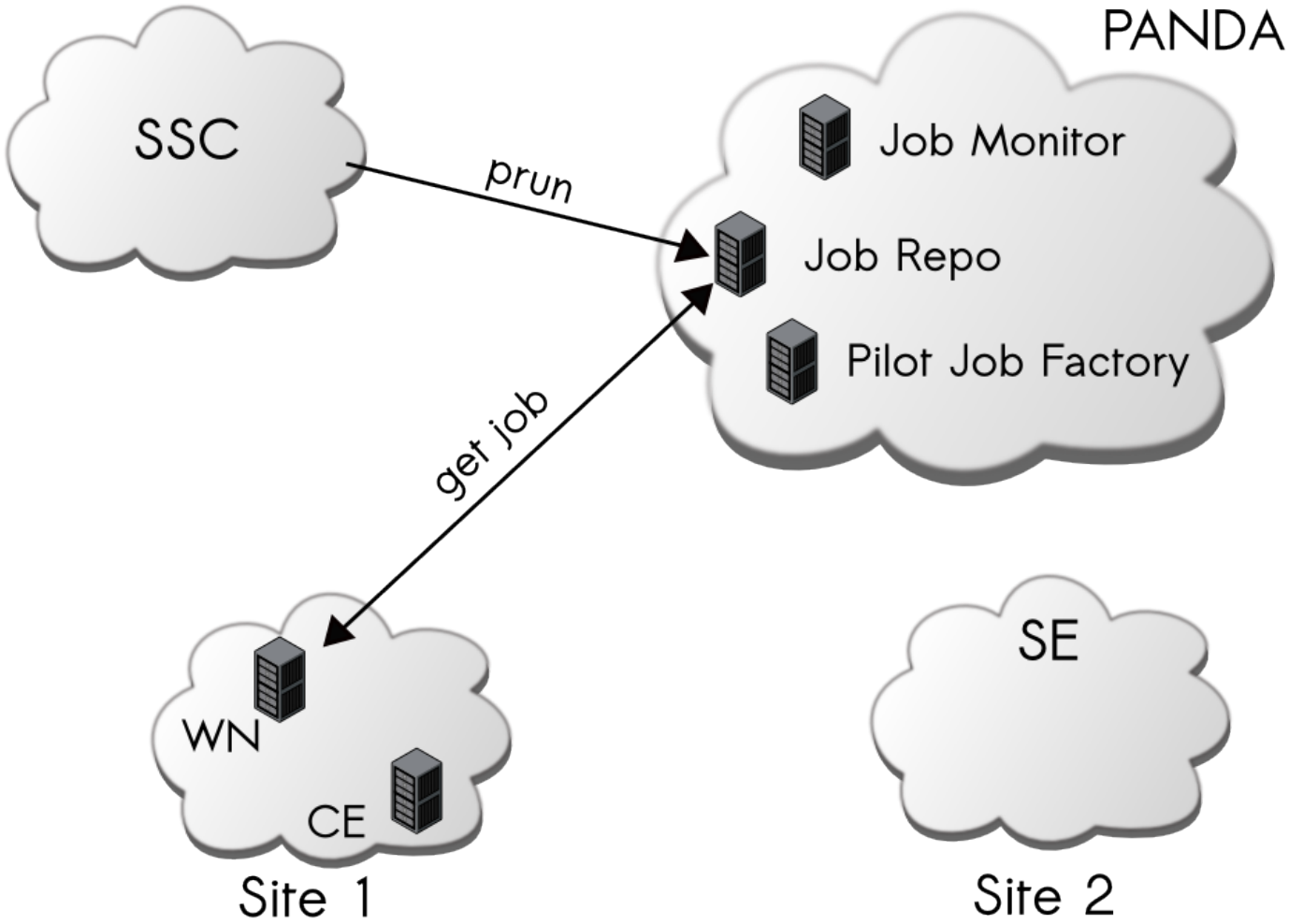
SSC-5 Layout



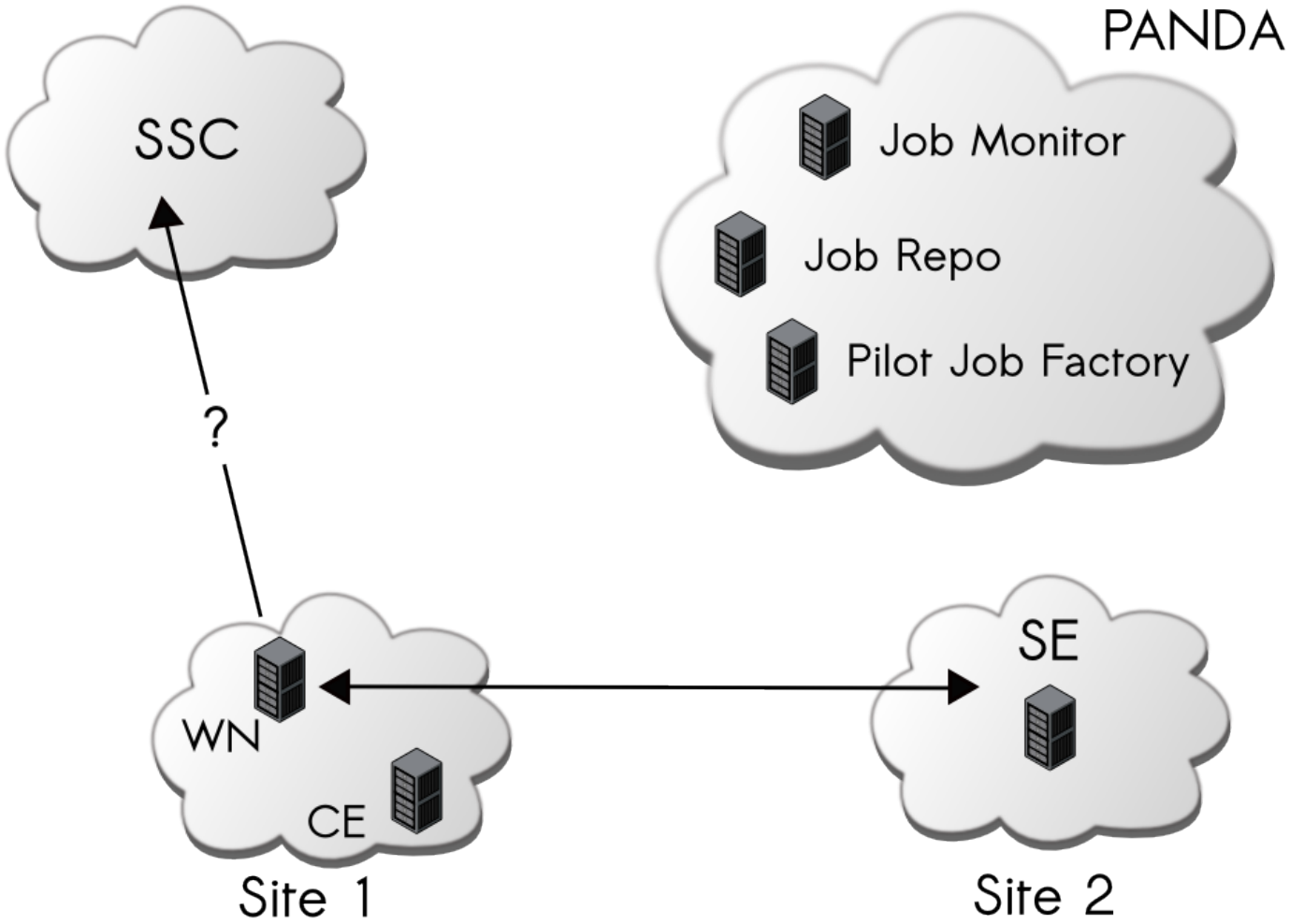
SSC-5 Layout


SSC
PANDA
Job Monitor
Job Repo
Pilot Job Factory
WN
CE
Site 1
SE
Site 2

SSC-5 Layout


PANDA
SSC
prun
Job Monitor
Job Repo
Pilot Job Factory
get job
WN
CE
Site 1
SE
Site 2

SSC-5 Layout


PANDA
SSC
Job Monitor
Job Repo
Pilot Job Factory
?
WN
CE
SE
Site 1
Site 2

Framework Status SSC-5 Prepara

- Negotiations with VO (Atlas) 100%
- Grid-Identity with access to VO-resources 100%
- Job-Submission framework 90% Sites will be added on request
- Malware: 95% currently debugging, done by Jeroen (Student at Nikhef).
- Database: 90% Missing integration of Storage Information
- RT-IR: 95 % Templates have to be finalized (input needed)
- Map: Display Info 80%
- Map: Trigger activity from Map (submit job, open ticket, ...) 80%
- User-Management Banning-monitor: communication to Monitor to be testet.

Demo

Todo

- Announcement/check communication within RT-IR (Dorine)
- Negotiations with sites to be done by NGIs
- Documentation of the Framework
- SSC the sites which are most often in Pakiti, SSC on demand

Evaluation/Expected Results

Current Evaluation Schema

- Communication
  - Heads-Up/Acknowledgement [4h]
  - Communication to VO [24h]
  - Notification of CA [144h]
  - Final-Report [144h]
- Containment
  - Stopped Malicious Job 4h]
  - Suspend User [8h]
  - Suspend Pilot-Job-Submitter [8h]
  - Unban Pilot-Job-Submitter [8h]
- Forensics
  - Find originating UI / (VO-)WMS [24h]
  - Analysis of the Network-Traffic [48h]
  - Analysis of Malicious Binary [48h]

Evaluation/Expected Results

Direct Monitor

- Response to initial ticket
- Found problematic Certificates
- Malicious Job stopped
- User Banned (Pilot-Job-User)
- Malicious binary contained and send to NGI
- Networkendpoints found/communicated

Added Objective: Managerial

The following questions should be answered:

- How much time would we have to spend on such an incident?
- How many sites fulfil our requirements (has to be defined: Response Times / Quality)?
- Which percentage of the overall resources would be affected?
- If this incident would have been real, how many sites would we have to block/suspend?