

# Security Service Challenges within the region

Ursula Epting, Sven Gabriel, Angela Poschlad

STEINBUCH CENTRE FOR COMPUTING - SCC



# Outline

- Goals of the Security Service Challenges
- Benefits for the regional security officer
- Benefits for the site administrators
  
- Execution of a SSC in ROC-DECH
  - Evaluation and feedback
  
- What did we learn?
- Conclusion

# Goals of the Security Service Challenges

- Testing the security skills in the region
  - Communication
    - Ensure that appropriate communication channels are available
  - Containment
    - Is information available to be able conducting an audit trace as part of a incident response
  - Forensics
  
- Raise a general interest and attention for security

# Benefits for the regional security officer

- Get an impression of knowledge/prioritization of and skills in security in the region
  - Who will be able to react in a responsible way in a real incident
  - Who probably will be unable to handle a real incident
  
- Also: A lot of work

## Benefits for the site administrators

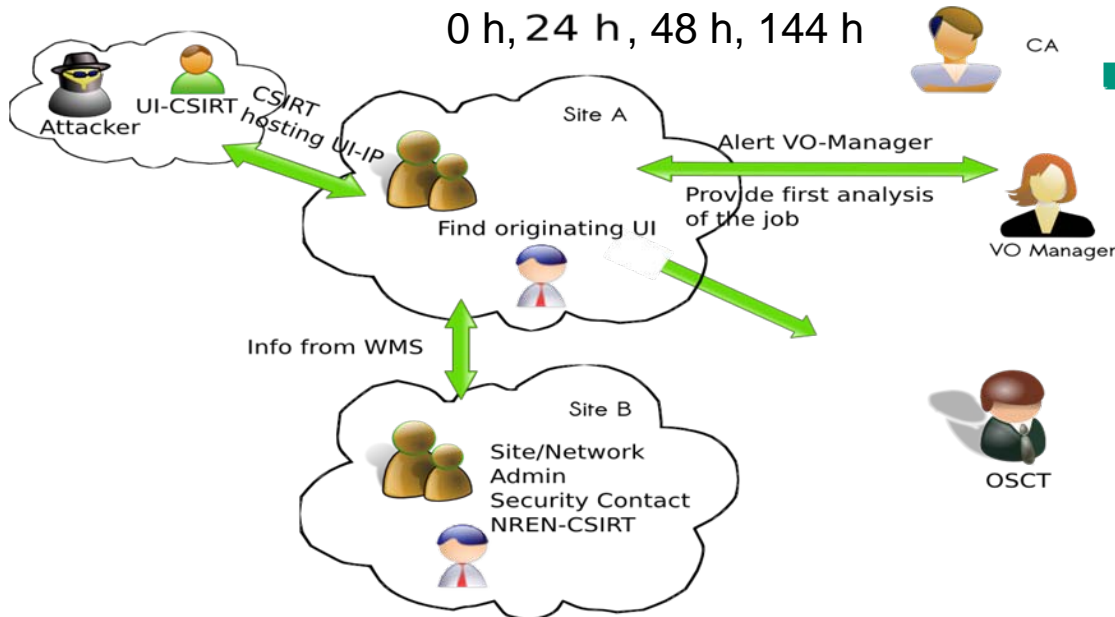
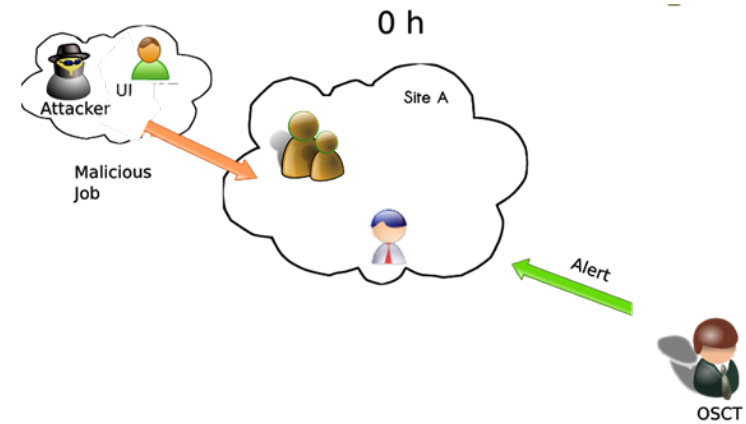
- Refresh knowledge of service interaction
  - Learn more about the own system
- Get familiar with the (EGEE) incident response procedures
- Test the internal communication channels and get used to each other, e.g. interaction with local CERT
  
- SSC gives feedback on the quality of reaction!
  - Hints where to gain more knowledge
  - Do I act as it is expected or even better?
  - Where do I have to learn more?

# Execution of a SSC in ROC-DECH

- I. Preparation and technical tests
  - Test the infrastructure for the challenge (computing, security lists)
  - Needs effort and time
  
- II. Inform the region
  - Inform about upcoming challenge
  - Provide information on incident response procedures
  
- III. Start of challenge
  
- IV. Evaluation

# Short overview on the Test

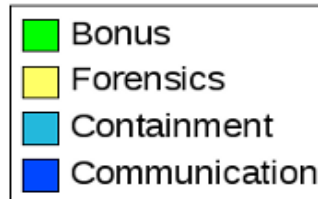
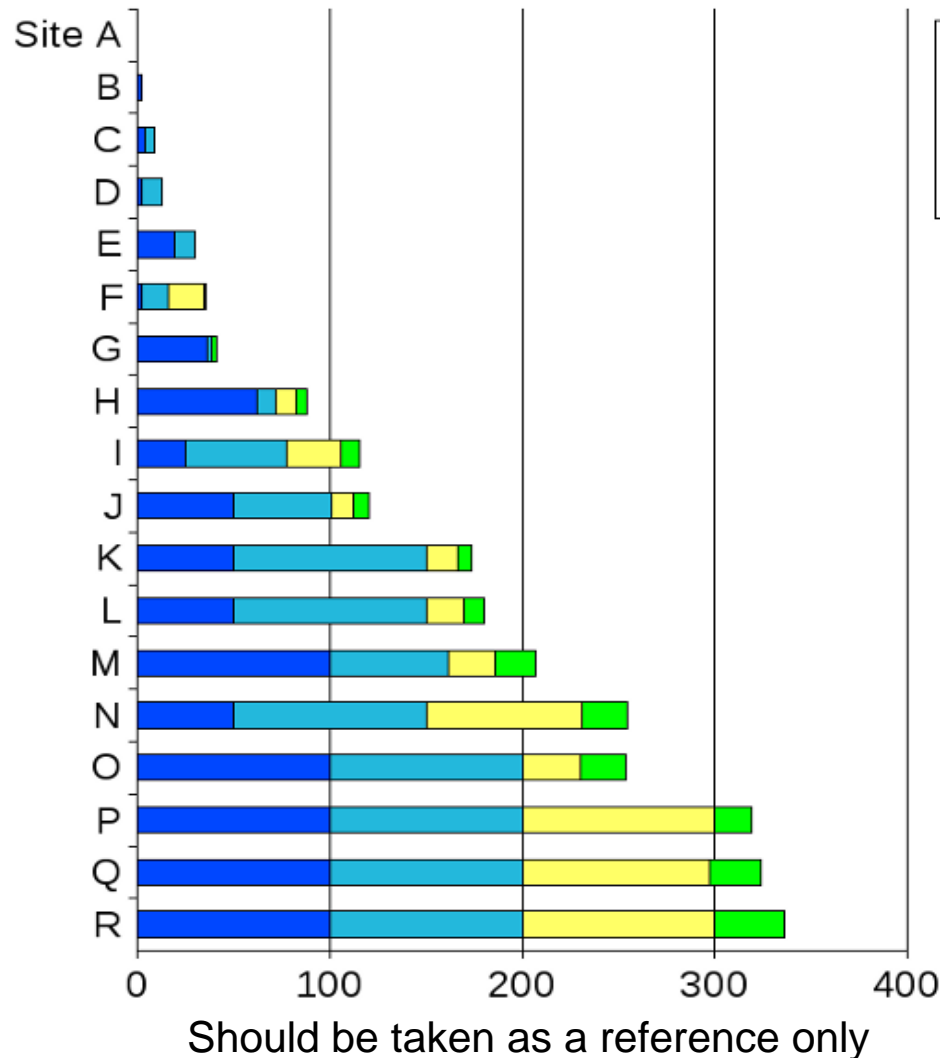
- “Malicious” job with legitimate grid credential sent to sites
  - Sites get informed by regional security officer



## ■ Several reactions expected after different time spans

- Acknowledgement and first actions (4h)
- Collecting information about incident and inform responsible units (24h)
- Analysis of malicious job (48 h)
- Final report to CSIRT (144h)

# Evaluation for the region Germany/Switzerland



- For communication, containment and forensics the maximum of 100 points were given each
- Bonus points could be gained for prompt reaction and good quality
- Average score in test
  - Communication: 47 points
  - Containment: 51 points
  - Forensics: 30 points



# What did go wrong?

- The main problem was the communication beginning with the email “THIS IS A TEST”
  - Misunderstanding as a not important email
  - Refusal of the test at two sites
  
- Site reinstalled WN after fake incident by hand
  - It would have been enough to say “If this was a real incident, we would now reinstall the WN”
  - Small sites do not have automatic installation procedures
  
- A manipulation of badly configured systems should be avoided
  - Check for vulnerability and not install e.g. a cron job

## Feedback from the sites

- Consideration as 'definitely', 'very' to 'moderately' useful
- Internal procedures will be adopted to integrate grid incidents into already existing procedures
- Most sites think they could score better in a next challenge, as more experience was gained now
- Several procedure documents which do not have all the same information were confusing
- Suggestion to add at least some links to best practice documents concerning user banning, machine forensics etc. since IRP does not provide any technical procedures – perhaps in form of a checklist
- Not full-time security specialists, so need of both time and instructions/manuals/howtos to dig into these topics
- Some sites question the necessity of Security Service Challenges as it puts additional workload on the involved people
- More site-to-site communication requested

## What did we learn?

- With an average of 51 points the containment shows that most sites are able to trace and kill jobs and suspend a user at the site – protection of own site
- 47 points for communication reflects the tendency to overlook the close relationship between all grid sites wide-spread over the world
- Only 30 point in forensic reveals a lack of security skills in the region
  
- Task has to be better communicated
- SSC identified the weakness in the current incident handling

# Conclusion

- SSC can be an important “tool” to fasten security knowledge and skills
- Challenge should be communicated more precisely
  - Especially the subject line should be changed to „Exercise“ or „challenge“ or „THIS IS A DRILL“ .
  - A bi-lingual introduction might lead to better communication
- The challenge showed a lack of security awareness
  - Single point for information required
- Forensic skills have to be strengthened
  - Links to best practice documents concerning user banning, machine forensics
  - Suggestion to have an email list for all security contacts and interested site admins to provide a platform for discussions on security concerns

# Thank you for your attention

STEINBUCH CENTRE FOR COMPUTING - SCC

