Summary

- Communication improved a lot. All sites send Heads-Up in time.
- Mail format/content improved.
- Some sites have user management problems.
- Many sites contacted atlas-cert.

Making use of the results - VO-WMS

- Available info not used (Panda-ID, URL).
- User-Interface not found by all sites
- Tools provided by some CERTS (KIT, Eygene).
- EGI-CSIRT Incident Response Procedure: Addendum Panda Involved
- Experiment-CSIRT: Procedure required to assure close collaboration with EGI-CSIRT in order to minimize impact on Service-availability

SSC4 – Next Steps

What Next

NGI-Runs/NDGF/OSG

- Run in NDGF and OSG if wanted.
- We could use Atlas/Panda in NGIs, but ...
- Scope/Evaluation revisited.
- Common report template needed to have the results comparable.
- How to get this in a traffic-light like representation of sites CSIRT performance.
- All communication SSC4-internal, mail templates (from EGI-CSIRT, Atlas-CERT, ...) needed.
- NGI Security Officer:
  - Negotiate with sites a date when to run. (1 or 2 weeks).
  - Do the Test-Incident-Coordination (with mail templates).
  - Monitor sites security operations with tools provided.
  - Timeline? This year?

EGI-CSIRT Challenge

- When NGI-Run finished, ...
- Over-next step: Big Run
  - Deploy Jobs to as many sites as possible; alert 1 smaller site.
  - Will show how we (EGI-CSIRT) collaborate, how the information propagates, how the incident gets contained.
- Iutra extended to execute commands on the client.
- Include Interested NRENs (might have other communication channels, approaches etc).

SSC4 – Next Steps

Open Discussion

Open Discussion Topics

- Security Monitoring: Service availability, in particular how do we communicate a service degradation.
- What should end up in our Request Tracker.
- Do we need a egi-csirt-discuss mailing list?
- Use of crypto in communications.(Leif)
- transits training for NGI/EGI security officers (Tobias)
- Some storage area to exchange saved disk images

Open Discussion Topics

- Can we quantify: patches and updates should be applied following best practice (roma.infn discussion).
- Romain: two approaches could help:
  - Suspend .. not patch within 7 days ... the EGI CSIRT marks critical ...
  - Publicly acknowledging (info to the VOs) those sites which are doing well (Pakiti may help)
  - Offer some optional EGI CSIRT security certification based on this, SSC results
- Ricardo:
  - ... whether our ”customers” would consider so much this kind of ”rating”. define some more levels .. than 2 (7 days, asap), example 1 or 2 months.
  - Remark Sven: Customars are rather VOs, afaik they are interested in security.
- Leif: baseline requirement ... **all** security patches must be