EGI-CSIRT Activities

Sven Gabriel, Nikhef, EGI-CSIRT

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142

EGI-CSIRT Activities

Sven Gabriel, Nikhef, EGI-CSIRT

Intro

- Logistics
- Agenda
- Last F2F

Intro

Agenda:

EGI-ENGAGE

Agenda

CERTIFIED BY TRUSTED INTRODUCER

Agenda: Thursday 8 Sept:

- Summary F2F Apr. 2016 Amsterdam, 15 min. (Sveng)
- CSIRT Web Appearance
- IRTF Debriefing/WLCG Traceability
- Lunch
- (Re-)Certification Procedures
- SOCs WLCG working group on Security Operations Centres
- SPG Update
- Trainings/SSC/SVG

Agenda

Agenda: Friday 9 Sept:

- Security Monitoring / Pakiti Deployment / RT-IR Update Status
- PY2 Planning

Intro

Logistics:

Logistics

- Coffee/Lunch served in the meeting room (11:00, 12:30, 15:00)
- Social Event: Dinner, Ian?

Logistics

- Minutes taking?

EGI-ENGAGE

Intro

CERTIFIED BY TRUSTED INTRODUCER

Recap: F2F 4 - 5 April, Amsterdam,:

Intro

Summary last F2F: SVG

- Report nr of Vulnerability tickets handled
- Report on Security Threat Risk Assessment
- FedCloud seen as highest risk - thinks that Enol is interested and engaged in improving.
- General discussion on Embassy clouds.
- DK: be part of WISE risk assessment group. DK: propose to distil to plans for work in year-2 of project.

Intro

Summary last F2F: RT Transition

- Transition finished.
- What is missing?
- Massticket framework still working?
- Report generation Tested?
- Access to tickets finer grained adjustable? (Site/NGI Security Officer)

Intro

Summary last F2F: Monitoring

- Pakiti - maintained by IRTF / Nagios - maintained by EGI monitoring group / Dash - maintained by dashboard devs.
- Who is coordinating this, under which mandate?
- What is the current integration status of these tools. (+ RT)
- How is the functionality monitored?
- Ready to hand over the housekeeping stuff to Operations? What is needed (automatation?)
- IanN: wants more compact view
- Sophie: more query options/ views
- Toby: feature request for pakiti.egi.eu -redirect to https!
- Sven: change "Pakiti-Check" test name to the CVE

Intro

Summary last F2F: IRTF

- Status Update on Vuln. Incidents
- Tools (pakiti, nagios stable, but slow) / Dashboard did not really work
- Massticket is fine, recommendation use Massticket as default to open tickets.
- SEC01 and SEC03 - what to do - the wiki provides more details on ’how to’
- Review SEC01/SEC03 during debriefing

Intro

Summary last F2F: IRTF Debriefing

- FedCloud Incident, contextuialistion fully broke the endporsement concept.
- A couple of open questions to FedCloud, see https://wiki.egi.eu/csirt/index.php/F2F_Amsterdam_4th_April_2016_PM
- Was this looked at? Perhaps put actions on IRTF members.
- UK Incident, basically OK, some tweaking in the handling process (delayed sending the closeout broadcast)

Intro

Summary last F2F: IRTF UKNGI Argus testing

- The repported success rate did not really match the expectations.
- Scripts in git?
- Redo this campaign?

Intro

Summary last F2F: Policies

- VM endorsment and operations
  - document is quite stable at the moment and considered done from our side
  - it is at OMB, but delayed - Peter S. asked for another two weeks for comments (must be finished before the review)
- Data protection policy
  - replacement of current accounting policy, generalized for all cases where personal data is processed
  - Peter S. - EGI works with lawyers and would like to include the results.... DaveK/G discussed this with people from EGI.

Intro

Summary last F2F: Policies contd

- IT infrastructure security policy
- current version was discussed
- davek will continure in development, collaboration welcome, continued in AARC

Intro

Summary last F2F: SSCs

- Aram got involved again
- next steps - integration with SSC monitoring, usage of contextualization

Intro

Summary last F2F: role-play-training at ISGC

- Report on RPT at ISGC
- We want to repeat elsewhere, possibly in AARC with real operators
- Scheduled for TI/TF-CSIRT meeting (Hannah), DI4R Krakow

Intro

Summary last F2F: ISGC paper

- decided not go for a paper we'll aim at next year or other opportunity (Chep)
- To be followed up here ...

Intro

Summary last F2F: EGI-CSIRT Wiki

- its still a mess
- agreed on a web presence (Ian, Sophie, Barbara)
- we need a plan to clean it up.
- To be followed up here, possibly in the session on the EH-CSIRT web page.
- same holds for the internal wiki

SSC

CERTIFIED BY TI TRUSTED INTRODUCER

SSC Update

SSC Update / Where I got stuck

- coordination problem/different timezones of developers

EGI-CSIRT Training activities

Training

- Defensive (Leif)

Projects: ISGC 2017 Paper