EGI-CSIRT Face2Face meeting in Amsterdam

Report of Contributions

https://indico.egi.eu/e/2900

Contribution ID: **0** Type: **not specified**

Status Update RT-IR

Presenter: KOURIL, Daniel (CESNET)

Contribution ID: **1** Type: **not specified**

Masstickets

How to go about this? Possible goal: be able to grab a list of all EGI-Critical vuln hosts out of Pakiti, drop it into a script, and presto, the script creates a ticket per site. Reasonable? There would be some prereqs:
* As reference, there must be a unified URL format, ideally something like https://wiki.egi.eu/wiki/EGI_CSIRT:Alerts/CVE-XXXX-YYYY. (I'd actually like to have the ability to find a given advisory by CVE number anyway.)
* A sensible general ticket template must be defined.
* The massmail script needs to be pimped a bit.

Presenter: Mr DUSSA, Tobias (KIT-CERT)

Contribution ID: **2** Type: **not specified**

RT-IR in IRTF, useage

RT-IR usage in IRTF, Discussion with Maintainer, what do we want to do with rt-ir, hww can this be done with rt-ir, what is needed / who does it

Presenter: BRILLAULT, Vincent (CERN)

Contribution ID: **3** Type: **not specified**

User/VM Management in FedCloud

Presenter: PARAK, Boris (CESNET)

Contribution ID: **4** Type: **not specified**

Integration to IRTF

Presenter: BRILLAULT, Vincent (CERN)

Contribution ID: **5** Type: **not specified**

VM Management/SSC

Needed bits fur SSC-FC
VM Management: Start/Stop/Contextualisation
How to get the SSC Payload into the VMs
What would be needed to control it from SSC-Monitor

Presenter: Dr GABRIEL, Sven (NIKHEF)

Contribution ID: **6** Type: **not specified**

SVG Update and Open Issues

Presenter: CORNWALL, Linda (STFC)

Contribution ID: **7** Type: **not specified**

Intro / Agenda

Presenter: Dr GABRIEL, Sven (NIKHEF)

Contribution ID: **8** Type: **not specified**

Security Policies update

Presenter: KELSEY, David (STFC)

Contribution ID: **9** Type: **not specified**

Security procedures updates

The evolution of operational security procedures, including forensics
Refine and extend the current security procedures and tools for incident response and forensics, for example: to take
into account new kinds of players (e.g. cloud resource providers), or to extend the emergency suspension mechanism to
cover new kinds of services. The security procedures related to other EGI operational procedures will also be modified
as required.

Presenter: BRILLAULT, Vincent (CERN)

Contribution ID: **10** Type: **not specified**

Procedures

Presenter: BRILLAULT, Vincent (CERN)

Contribution ID: **11** Type: **not specified**

Welcome, introduction, agenda, note takers, logistics etc

Monday, 4 April 2016 09:00 (30 minutes)

Presenter: Dr GABRIEL, Sven (NIKHEF)

Session Classification: Session 1

Contribution ID: **12** Type: **not specified**

SVG issues and Risk Assessment (SCG)

Monday, 4 April 2016 09:30 (1 hour)

Report and discussion on Security Threat Risk Assessment.
outcomes - what we are doing or need to do to address the main areas of concern.
Monitoring other than the WN. Some vulnerabilities are considered 'Critical' in some cases, but not 'Critical' on the WN, which is all that can be monitored at present. Is there anything better that can be done?

Presenter: CORNWALL, Linda (STFC)

Session Classification: Session 1

Contribution ID: **13** Type: **not specified**

Security Monitoring

Monday, 4 April 2016 11:00 (1h 30m)

Update on RT-IR
Update on pakiti, security dashboard
How to use the tools as Security Officer on Duty

Presenter: KOURIL, Daniel (CESNET)

Session Classification: Session 1

Contribution ID: **14** Type: **not specified**

IRTF part 1

Monday, 4 April 2016 14:00 (1h 30m)

Presentation - expectations of the officer on duty
(15 minutes presentation, 15 minutes discussions?)
Massticket-tool (as part of How to use the tools as Security Officer on Duty
Input from: (Daniel/Ian/Vincent/Toby)
Basic presentation on how to use mass ticket
Discuss on how to improve the template/make it simpler
15 minutes presentation, 30 minutes discussion?
Central Banning Update from Vincent
- (IanN) testing UK-argus banning system
if Ian has tested it, a report on testing the UK ngi-central
banning system. (related to ticket 10171)

Presenters: KOURIL, Daniel (CESNET); Mr NEILSON, Ian (STFC); Mr DUSSA, Tobias (KIT-CERT); BRILLAULT, Vincent (CERN)

Session Classification: Session 2

Contribution ID: **15** Type: **not specified**

IRTF part 2

Monday, 4 April 2016 16:00 (1 hour)

Debriefing for EGI-20160228-01
Less than 15 minutes, this is a simple incident
Debriefing for EGI-20160301-01
At least 15 minutes? Quite few complications. Output interesting for Fedcloud part of the meeting

Presenter: BRILLAULT, Vincent (CERN)

Session Classification: Session 2

Contribution ID: **16** Type: **not specified**

Agenda review

Tuesday, 5 April 2016 09:00 (10 minutes)

Session Classification: Session 3

Contribution ID: **17** Type: **not specified**

Security policies

Tuesday, 5 April 2016 09:10 (50 minutes)

Brief update of status of new/revised policies.
Policies to be updated in 2016.
Some word-smithing on one policy (if time?)

Presenter: KELSEY, David (STFC)

Session Classification: Session 3

Contribution ID: **18** Type: **not specified**

EGI-Engage SA1.2

Tuesday, 5 April 2016 10:00 (30 minutes)

Reminder of what happened in PY1.
Roadmap for PY2 (starting 1 March 2016).

Presenter: KELSEY, David (STFC)

Session Classification: Session 3

Contribution ID: **19** Type: **not specified**

EGI FedCloud Security

Tuesday, 5 April 2016 14:00 (1h 30m)

VB (15 min + 15 min Discussion) Incident Response in FedCloud
-summary of Cloud incidents, what is working well, what not, what is missing
(30 min + Discussion) EGI Federated Cloud improvement plan (focus on security)
Sveng: RP Certification Procedure (15 min Presentation 15 min Discussion)
Discussion VM/User Management beyond OpenNebula (Boris)
Automated security checks done by CZ (Daniel)

Presenters: PARAK, Boris (CESNET); KOURIL, Daniel (CESNET); Dr FERNANDEZ, Enol (EGI.eu); Dr GABRIEL, Sven (NIKHEF); BRILLAULT, Vincent (CERN)

Session Classification: Session 4

Contribution ID: **20** Type: **not specified**

AOB, wrap-up

Tuesday, 5 April 2016 16:30 (30 minutes)

Session Classification: Session 4

Contribution ID: **21** Type: **not specified**

Update on SSC

Tuesday, 5 April 2016 11:00 (30 minutes)

Presenter: Dr GABRIEL, Sven (NIKHEF)

Session Classification: Session 3

Contribution ID: **22** Type: **not specified**

News from ISGC2016, EGI CSIRT web & wiki

Tuesday, 5 April 2016 11:30 (30 minutes)

Presenter: Dr GABRIEL, Sven (NIKHEF)

Session Classification: Session 3

Contribution ID: **23** Type: **not specified**

Plans for next meetings

Tuesday, 5 April 2016 12:00 (30 minutes)

Session Classification: Session 3

Contribution ID: **24** Type: **not specified**

EGI FedCloud Security (continued)

Tuesday, 5 April 2016 16:00 (30 minutes)

Session Classification: Session 4