EGI-CSIRT Face2Face meeting in Prague

Report of Contributions

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

RT-IR Status

Presenter: STAVA, Michal (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**

EGI Security Threat Risk Assessment

Security requirements and risk assessment for new services, technology, and deployments
The new developments and evolving usage scenarios in EGI-Engage will involve trust models different from the core
infrastructure used in EGI-InSPIRE. The task will ensure that the security requirements and the trust model are defined.
Any security problems will be addressed and risk assessment associated with new deployments will be developed, to
drive operational security in the evolved environment, to keep services secure and available and to mitigate the serious
risks

Presenter: CORNWALL, Linda (STFC)

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

Intro / Agenda

Tuesday, 17 January 2017 13:00 (30 minutes)

Presenter: Dr GABRIEL, Sven (NIKHEF)

Session Classification: Intro

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

Security Policy update and issues

Develop a new trust framework and develop new policies
In collaboration with other infrastructures, we will define new additions to a new policy framework to handle the new
deployment and usage scenarios as they evolve in EGI-Engage.

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**

IPv6 Security

Presenter: KELSEY, David (STFC)

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

VB IRTF Mandate, duty rota and future

Wednesday, 18 January 2017 18:00 (30 minutes)

Presenter: BRILLAULT, Vincent (CERN)

Session Classification: IRTF

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

VB Procedures for introduction SUID binary?

Wednesday, 18 January 2017 15:00 (25 minutes)

Presenter: BRILLAULT, Vincent (CERN)

Session Classification: Random Stuff

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

VB Security contact mailing list

Wednesday, 18 January 2017 14:45 (15 minutes)

Presenter: BRILLAULT, Vincent (CERN)

Session Classification: Random Stuff

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

Venom Rootkit

Tuesday, 17 January 2017 16:00 (30 minutes)

Presenter: KOURIL, Daniel (CESNET)

Session Classification: IRTF

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

Debriefing

Tuesday, 17 January 2017 16:30 (1 hour)

Presenters: KOURIL, Daniel (CESNET); Dr GABRIEL, Sven (NIKHEF); BRILLAULT, Vincent (CERN)

Session Classification: IRTF

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

ISGC CSIRT Presentation

Wednesday, 18 January 2017 09:00 (30 minutes)

Presenter: Dr GABRIEL, Sven (NIKHEF)

Session Classification: ISGC

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

ISGC Fyodor

Wednesday, 18 January 2017 09:30 (30 minutes)

Presenter: YAROCHKIN, Fyodor (AS)

Session Classification: ISGC

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

ISGC Training

Wednesday, 18 January 2017 10:00 (30 minutes)

Presenter: Dr GABRIEL, Sven (NIKHEF)

Session Classification: ISGC

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

Enhanced privacy for security-related GGUS tickets

Wednesday, 18 January 2017 14:00 (15 minutes)

… evaluate the possibility for security officers to open GGUS tickets for selected sites, informing them on sensitive information (poorly configured services, urgent patches, etc) so, such tickets should remain more private than the rest.

Today, GGUS ticket viewing requires a valid certificate from a trusted CA AND also to be a registered GGUS user. Also, GGUS tickets are not googleable, except for some fora who decided to use google groups (don't ask me why‼!???) e.g. https://groups.google.com/forum/#!topic/argus-support/gWDksPP5P5s

Still, the security officers, to integrate security and operations (and not use the EGI RT) would like the list of DNs allowed to track such GGUS tickets to be more restricted.

…

Presenters: Mr NEILSON, Ian (STFC); BRILLAULT, Vincent (CERN)

Session Classification: Random Stuff

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

Argus monitoring

Wednesday, 18 January 2017 14:15 (30 minutes)

The argus framework was never tested on a project level.
Start project to test the that the banning info ends up at the CEs/WMSs/in the VO-WMSes (Panda, CRAB etc)
banning Issues with the storage systems.

Presentation: IanN,Status update from UK on testing argus

Presenters: Mr NEILSON, Ian (STFC); BRILLAULT, Vincent (CERN)

Session Classification: Random Stuff

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

IRTF Mandate, duty rota and future

Goals: Making IRTF more productive for Incident Response and stop doing non-interesting stuff

Presenter: BRILLAULT, Vincent (CERN)

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

Procedures for introduction SUID binary

Presenter: BRILLAULT, Vincent (CERN)

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

Security contact mailing list

Presenter: BRILLAULT, Vincent (CERN)

Contribution ID: **25** Type: **not specified**

SVG

Presenter: CORNWALL, Linda (STFC)

Contribution ID: **26** Type: **not specified**

Security Monitoring /Dashboard Status Update

Wednesday, 18 January 2017 16:30 (30 minutes)

Status of the IRTF tools:
- Security Dashboard
- RT-IR
- Massticket system
- Single Ticket mode

Presenters: KOURIL, Daniel (CESNET); BRILLAULT, Vincent (CERN)

Session Classification: IRTF

Contribution ID: **27** Type: **not specified**

IR in FedCloud, preparation session

Wednesday, 18 January 2017 17:00 (1 hour)

- Prepare for the Session with FedCloud on Thursday
- With who do we communicate
- Do we treat FedCloud Users as Admins? (Trustwise, i.e. add them to the ticket?)
- What is the role of the VO here?
- Note: we may see situations, were users set up compute clusters in the cloud, to be used by multiple people from a vo
- Note 2: we may see situations, were users set up compute clusters in the cloud, to be used by individuals with which we have no connection what-so-ever

Presenter: BRILLAULT, Vincent (CERN)

Session Classification: IRTF

Contribution ID: **28** Type: **not specified**

Trainings in EGI

Wednesday, 18 January 2017 11:00 (1 hour)

Presenter: Dr GABRIEL, Sven (NIKHEF)

Session Classification: ISGC