EGI-CSIRT Face2Face meeting in Lisbon

Report of Contributions

https://indico.egi.eu/e/3347

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

Enhanced privacy for security-related GGUS tickets

… 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)

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

Argus monitoring

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)

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

VB Security contact mailing list

Presenter: BRILLAULT, Vincent (CERN)

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

VB Procedures for introduction SUID binary?

Presenter: BRILLAULT, Vincent (CERN)

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

ISGC CSIRT Presentation

Presenter: Dr GABRIEL, Sven (NIKHEF)

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

ISGC Fyodor

Presenter: YAROCHKIN, Fyodor (AS)

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

ISGC Training

Presenter: Dr GABRIEL, Sven (NIKHEF)

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

Trainings in EGI

Presenter: Dr GABRIEL, Sven (NIKHEF)

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

Intro / Logistitcs / Agenda

Thursday, 18 May 2017 09:00 (30 minutes)

Presenter: Dr GABRIEL, Sven (NIKHEF)

Session Classification: Intro

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

Venom Rootkit

Presenter: KOURIL, Daniel (CESNET)

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

Debriefing

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

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

Security Monitoring /Dashboard Status Update

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

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

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

IR in FedCloud, preparation session

- 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)

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

VB IRTF Mandate, duty rota and future

Presenter: BRILLAULT, Vincent (CERN)

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

VO Security Communication Challenge

Presenter: BRILLAULT, Vincent (CERN)

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

WLCG Traceability & Isolation WG report

Presenter: BRILLAULT, Vincent (CERN)

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

How to Contact users

Clarify procedures (VOs, AAI check-in, robots)
Discussion: Problem with Robot Certificates (GoeGrid Incident)
Describe Problem, check if this is a policy violation, escalate to Management (via OMB)

Presenter: BRILLAULT, Vincent (CERN)

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

GoeGrid Issues / How to Contact Users

Thursday, 18 May 2017 16:00 (30 minutes)

Clarify procedures (VOs, AAI check-in, robots)
Discussion, identify possible policy violations of the users/VO, escalate to Management via OMB

Presenter: BRILLAULT, Vincent (CERN)

Session Classification: IRTF

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

VM image handing in IR

Thursday, 18 May 2017 16:30 (45 minutes)

Concept to use syncthing to share VM images, what is needed at the sites, what at irtf. POC, then ask OMB for approval/support

Presenter: Mr DUSSA, Tobias (KIT-CERT)

Session Classification: IRTF

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

Critical Vulnerability Handling Handover to Operations

Questions that I see are:
- Monitoring: How to make sure that Operations people are allowed to see the relevant info.
- Is the info there distinct enough so that they don't trap into false positives/mitigations/etc, what do we need to do in terms of training/documentation?

- Ticket creation still be done by us (Massticket Magic)
- Low level tech communications (Advisories etc) should be done by us. In addition we may need to provide support (on Duty dude has to provide this)

For now we can assume that we use our tools, no need to move to ggus atm.

Peter will be available/dial in on Friday (mainly for the FedCloud Sec stuff) perhaps we can through this at him as well, and get to a point where we can present this at OMB and ask for approval.

Can you guys collect/present the needed info so that we can discuss it. Only very brief, likely we can re-use some of the Prague stuff we had back then.

Security Monitoring may need some more love here.

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

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

Handover discussion

Friday, 19 May 2017 11:00 (15 minutes)

Questions that I see are:
- Monitoring: How to make sure that Operations people are allowed to see the relevant info.
- Is the info there distinct enough so that they don't trap into false positives/mitigations/etc, what do we need to do in terms of training/documentation?

- Ticket creation still be done by us (Massticket Magic)
- Low level tech communications (Advisories etc) should be done by us. In addition we may need to provide support (on Duty dude has to provide this)

For now we can assume that we use our tools, no need to move to ggus atm.

Peter will be available/dial in on Friday (mainly for the FedCloud Sec stuff) perhaps we can through this at him as well, and get to a point where we can present this at OMB and ask for approval.

Can you guys collect/present the needed info so that we can discuss it. Only very brief, likely we can re-use some of the Prague stuff we had back then.

Security Monitoring may need some more love here.

Session Classification: IRTF