

# **EGI-CSIRT Face2Face meeting in Abingdon**

## **Report of Contributions**

Contribution ID: 0

Type: **not specified**

## **Introduction, Last meeting, Agenda, note takers, logistics etc**

*Thursday, 8 September 2016 09:30 (20 minutes)*

**Presenter:** Dr GABRIEL, Sven (NIKHEF)

**Session Classification:** Welcome\_Logisitcs\_Last\_Meeting

Contribution ID: 1

Type: **not specified**

## **SVG issues and Risk Assessment (SCG)**

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)

Contribution ID: 2

Type: **not specified**

## Security Monitoring

Update on RT-IR

Update on pakiti, security dashboard

How to use the tools as Security Officer on Duty

**Presenter:** KOURIL, Daniel (CESNET)

Contribution ID: 3

Type: **not specified**

## IRTF part 1

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); BRIL-  
LAULT, Vincent (CERN)

Contribution ID: 4

Type: **not specified**

## IRTF part 2

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)

Contribution ID: 5

Type: **not specified**

## EGI FedCloud Security

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)

Contribution ID: 6

Type: **not specified**

## **EGI FedCloud Security (continued)**



Contribution ID: 7

Type: **not specified**

## **AOB, wrap-up**

*Friday, 9 September 2016 14:00 (30 minutes)*

**Session Classification:** WrapUp Actions Next Meeting

Contribution ID: 8

Type: **not specified**

## Agenda review

Contribution ID: 9

Type: **not specified**

## Security policies

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)

Contribution ID: **10**

Type: **not specified**

## **EGI-Engage SA1.2**

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

**Presenter:** KELSEY, David (STFC)

Contribution ID: **11**

Type: **not specified**

## **Update on SSC**

**Presenter:** Dr GABRIEL, Sven (NIKHEF)

Contribution ID: 12

Type: **not specified**

## **News from ISGC2016, EGI CSIRT web & wiki**

**Presenter:** Dr GABRIEL, Sven (NIKHEF)

Contribution ID: 13

Type: **not specified**

## Plans for next meetings

Contribution ID: 14

Type: **not specified**

## **PY2 Planning**

*Friday, 9 September 2016 13:30 (30 minutes)*

Wrap up Discussion on PY2 planning

**Presenter:** KELSEY, David (STFC)

**Session Classification:** WrapUp Actions Next Meeting



Contribution ID: 15

Type: **not specified**

## **PY2 Planning**

15 min Presentation of the proposal draft send in on 7th Sept  
Discussion, what can we add, what do we want to do, what are the priorities

**Presenter:** KELSEY, David (STFC)

Contribution ID: **16**

Type: **not specified**

## Monitoring

*Friday, 9 September 2016 09:10 (1h 20m)*

**Presenter:** KOURIL, Daniel (CESNET)

**Session Classification:** Security Monitoring

Contribution ID: 17

Type: **not specified**

## CSIRT Web-Page

**Presenters:** KRASOVEC, Barbara (ARNES); Mr NELSON, Ian (STFC); FERRY, Sophie (CEA)

Contribution ID: **18**

Type: **not specified**

## **Incidents Debriefing**

**Presenter:** BRILLAULT, Vincent (CERN)

Contribution ID: 19

Type: **not specified**

## **Pakiti Deployment**

*Friday, 9 September 2016 10:30 (20 minutes)*

**Presenter:** BRILLAULT, Vincent (CERN)

**Session Classification:** Security Monitoring

Contribution ID: 20

Type: **not specified**

## **SOCs WLCG working group on Security Operations Centres**

*Thursday, 8 September 2016 14:00 (20 minutes)*

**Presenter:** Mr NELSON, Ian (STFC)

**Session Classification:** SPG/IRTF Site Certification Procedure / Pakiti Deployment / SOC's

Contribution ID: 21

Type: **not specified**

## **Debriefing EGI-20160509-01**

*Thursday, 8 September 2016 11:30 (30 minutes)*

**Presenter:** BRILLAULT, Vincent (CERN)

**Session Classification:** IRTF Debriefing/WLCG Traceability

Contribution ID: 22

Type: **not specified**

## **WLCG Traceability & Isolation**

*Thursday, 8 September 2016 12:00 (30 minutes)*

**Presenter:** BRILLAULT, Vincent (CERN)

**Session Classification:** IRTF Debriefing/WLCG Traceability



Contribution ID: 23

Type: **not specified**

## Certification Procedures

*Thursday, 8 September 2016 13:30 (30 minutes)*

**Presenter:** Dr GABRIEL, Sven (NIKHEF)

**Session Classification:** SPG/IRTF Site Certification Procedure / Pakiti Deployment / SOCs

Contribution ID: 24

Type: **not specified**

## Welcome Logistics Events

*Thursday, 8 September 2016 09:00 (30 minutes)*

**Presenters:** KELSEY, David (STFC); Mr NEILSON, Ian (STFC)

**Session Classification:** Welcome\_Logisitcs\_Last\_Meeting

Contribution ID: 25

Type: **not specified**

## **SVG, Status update**

**Presenter:** CORNWALL, Linda (STFC)

Contribution ID: 26

Type: **not specified**

## HepSysMan Training

*Thursday, 8 September 2016 15:50 (20 minutes)*

**Presenter:** Mr NELSON, Ian (STFC)

**Session Classification:** Trainings\_SSC\_SVG

Contribution ID: 27

Type: **not specified**

## **Training Portfolio / RPT / Offensive / Defnsive**

*Thursday, 8 September 2016 15:30 (20 minutes)*

**Presenter:** Dr GABRIEL, Sven (NIKHEF)

**Session Classification:** Trainings\_SSC\_SVG

Contribution ID: 28

Type: **not specified**

## SVG

*Thursday, 8 September 2016 16:30 (30 minutes)*

**Presenter:** CORNWALL, Linda (STFC)

**Session Classification:** Trainings\_SSC\_SVG

Contribution ID: 29

Type: **not specified**

## **SPG Update**

*Thursday, 8 September 2016 14:40 (20 minutes)*

**Presenter:** KELSEY, David (STFC)

**Session Classification:** SPG/IRTF Site Certification Procedure / Pakiti Deployment / SOCs

Contribution ID: **30**

Type: **not specified**

## **RTIR Updates**

*Friday, 9 September 2016 09:00 (10 minutes)*

**Presenter:** KOURIL, Daniel (CESNET)

**Session Classification:** Security Monitoring



Contribution ID: **31**

Type: **not specified**

## **TLP Updated definitions**

*Thursday, 8 September 2016 16:10 (20 minutes)*

**Presenter:** Dr GABRIEL, Sven (NIKHEF)

**Session Classification:** Trainings\_SSC\_SVG

Contribution ID: **32**

Type: **not specified**

## **EGI-CSIRT Web**

*Thursday, 8 September 2016 09:50 (20 minutes)*

**Presenters:** KRASOVEC, Barbara (ARNES); Mr NELSON, Ian (STFC); FERRY, Sophie (CEA)

**Session Classification:** CSIRT Web Appearance