#15

COMPLETE

Collector:	Web Link 1 (Web Link)
Started:	Friday, February 09, 2018 7:11:15 PM
Last Modified:	Friday, February 09, 2018 7:16:31 PM
Time Spent:	00:05:15
IP Address:	130.246.41.121

Page 1: Report on performance of the service

Q1 Service

Security coordination and security tools

Q2 The reporting person:

Name	**David Kelsey (STFC)**
E-mail	**david.kelsey@stfc.ac.uk**

Q3 EFFORT(Please provide effort (PM) spent by each partner (separately) during the whole reporting period.)

During these 6 months we all spent at least according to the allocations. In addition, the partners provided additional (funded or unfunded) effort not reported here. The allocations (and hence spend) are as follows:

CERN 2.5 PM
CESNET 2 PM
GRNET 0.8 PM
Nikhef 3.5 PM
STFC 4 PM

TOTAL 12.8 PM

Q4 GENERAL OVERVIEW OF ACTIVITY IN THE PERIOD(Short prose overview of what happened in the period. Things went well? There were problems but they were addressed? There were significant problems that persist and must be dealt with?)

The Security Coordination and Security Tools functions performed well during another busy period for operational security. Coordination activities were carried out as expected in collaboration with EGI-Engage (until 31st August) including regular weekly/monthly/face to face meetings and active participation in events. Reports were presented at the monthly EGI OMB meetings. A CSIRT F2F meeting was held in Helsinki (15-17 Nov). An SPG F2F meeting was held jointly with AARC2 in Amsterdam on 5-7 July.

EGI was represented and members of the team played leading roles at many different meetings, including TF-CSIRT in Stockholm (19-22 Sep), FIRST meeting (summer, Costa Rica) SIG-ISM in Brussels (5-6 Oct), WISE in Arlington VA combined with NSF CyberSecurity summit (15-17 Aug).

Sven Gabriel (EGI Security Officer) was elected in September to the TF-CSIRT Steering Committee for the next 3 years.

Coordination of IRTF continued and handled 3 (suspected) security incidents: [EGI-20170825], [EGI-20171101], and [EGI-20171213].

The number of RT-IR tickets created and handled in the period was 76. Just two GGUS tickets were handled during the period, well within the SLA-defined time limits.

This was a busy time for the SVG Issue handling with 23 new issues reported. This includes 2 assessed as 'Critical' risk and 2 'High' risk. 13 advisories were issued on the public wiki. The updating of the issue handling procedure in collaboration with EGI-Engage was completed and approved by OMB in November.

SPG, in collaboration with EGI-Engage and AARC2, at its F2F meeting in July produced updated policy documents, including two draft Community policy documents. These were presented to OMB twice and finalised/approved in November. These are still waiting formal approval by the EB and adoption.

The trust anchor distribution was updated monthly as required. Chaired EUGridPMA/IGTF All Hands meeting in Manchester (25-27 Sep). EGI was represented in the IGTF F2F meetings in Asia/Pacific (15 Oct). No F2F meeting of TAGPMA was held during the period.

The results of EGI security monitoring were used to reveal issues and provide support for on-duty members of EGI-CSIRT so that sites could be contacted and asked for actions. Several certification requests were addressed over the reporting period.

Participated in WISE Steering committee meetings. SCI version 2 was reviewed at the WISE meeting in Arlington (15 Aug).

Talks were given at the DI4R conference in Brussels (29-30Nov).

In collaboration with EGI-Engage, the FedCloud Security Service Challenge was run in July-August. Results were analysed and lessons learned.

Q5 ISSUES ARISING IN THE PERIOD(Explain issues, such as OLA violations or other problems in performance. Also consider other events that may not lead to violations, such as planned downtime, or problems in services there is a dependency on.)

As reported previously, the security monitoring framework relies on old versions of monitoring tools that are not supported, which puts the monitoring infrastructure at risk. This has been true for a long time and its importance is now critical.

Q6 MITIGATION ACTIONS PLANNED (Explain action planned to mitigate issues in this period.)

SECMON: We started evaluation of needs for transition to a new framework some time ago. The actual move will need the additional resources which were planned for EOSC-Hub.

Q7 FORESEEN ACTIVITIES AND CHANGES (Note upcoming activities or changes impacting the service and OLA that are the subject of this report. For instance planned ending or renegotiation of the agreement or planned major upgrades to the service, new activities.)

Operational security activities will continue. We, in collaboration with EOSC-hub, will prepare for and run when ready, a security drill on DIRAC job submission system. In the EOSC-Hub era we will have closer collaboration with other Infrastructures, especially with EUDAT. There will be an EGI CSIRT/EUDAT F2F meeting at CERN on 29-31 Jan 2018 when we will start the work of harmonising policies and procedures. Full details of the many aspects of our work in EOSC-hub are documented elsewhere. There will be a WISE workshop in Abingdon UK hosted by STFC on 26-28 Feb.