#6

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Tuesday, September 20, 2016 12:14:18 PM
Last Modified: Tuesday, September 20, 2016 12:18:10 PM
Time Spent: 00:03:52
IP Address: 128.141.7.128

PAGE 1: Report on performance of the service

Q1: **Service**	Security coordination and security tools

Q2: **The reporting person:**

Name	David Kelsey
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 4 months we all spent at least according to the allocations. In addition many partners provided additional (funded or unfunded) effort not reported here.

CERN	1.67 PM
CESNET	1.33 PM
GRNET	0.67 PM
Nikhef	2.33 PM
STFC	2.67 PM
TOTAL	8.67 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 a busy period for operational security. Coordination activities were carried out as expected in collaboration with EGI-Engage including regular weekly/monthly/face to face meetings and active participation in events. Operational security coordination in the EGI CSIRT and preparation for the extension of our TF-CSIRT accreditation is an ongoing effort. EGI was here represented at the FIRST conference and TF-CSIRT meetings. Planning for CSIRT F2F meeting in Abingdon (Sep).

Three multi-site security incidents were handled (involving more than 30 sites). There were several campaigns chasing patching of the infrastructure to fix critical vulnerabilities. The number of RT-IR tickets created and handled in the period was 124. One multi-site security incident (in May) revealed minor internal coordination issues for which a solution will now be tested, but also a more problematic conceptual issue with the EGI FedCloud.

This was a busy time for the SVG Issue handling, 19 new issues were reported during these 4 months. This includes 3 assessed as 'Critical' risk and 3 'High' risk.   14 advisories were issued on the public wiki.

The trust anchor distribution was updated two times. Preparation for the inclusion of the on-line "IOTA" CA was completed, but its implementation is still awaiting necessary updates to deployed access control software and endorsement of the accompanying policy. Hosted EUGridPMA meeting in Abindgon (May). EGI was represented in the IGTF F2F meetings in the Americas (during the XSEDE conference).

During this period the SECMON service was migrated from the infrastructure at AUTH to the ~okeanos cloud infrastructure. The migration started in May and was completed in July. The SECMON team handled 7 GGUS tickets, including 4 re-certifications.

Evaluation of results produced by security probes and issues detected. Supporting on-duty members of EGI-CSIRT with monitoring needs.
- Pakiti configuration improved to better use database engine and better distinguish among different sources of data
- Addressing several certification requests (3), one is still open due to the need to clarify the state of tools available.

WISE Steering committee meetings, Co-chaired WISE meeting in Miami (July), prepared for WISE workshop in Krakow (September). Leadership of WISE SCIV2-WG. Chaired meetings and worked on next version of SCI document. Member of DI4R Programme Committee.

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.)

IRTF is relying on the Security Monitoring, which has had a few issues in August. These issues revealed that the future of this service, which relies on deprecated software, is worrisome and migration to more supported software should be considered.
The security incident in May has shown again that the EGI FedCloud, especially for sites that do not restrict incoming network activity by default, can lead to basic security issues, that we would not expect on well maintained modern sites... (for example world-writable NFS exports,
default basic passwords).

As well as a higher number of issues to handle than usual, some have not been straight forward and have required a lot of work, as well as happening at a time when people are taking a lot of holidays. One critical issue has been a bit slower than we would have liked to get resolved. This has also meant some other activities have not progressed as much as anticipated.

There are no known issues or SLA violations for operational security coordination or trust anchor management.

SECMON issues:

1. The budget available for the operation of the secmon service has been significantly reduced. For the next period, there is no foreseen effort for probe maintenance and evolution of the service. This is closely related to points 2 and 4.

2. The personnel responsible for the operation and maintenance of the secmon had to be reallocated due to the budget redactions. The team changes along with the necessary migration to the ~okeanos infrastructure, resulted in consuming 45% of the yearly budget in the first 4 months.

3. Secmon relied on the certification infrastructure in order to monitor uncertified sites during the certification process. On July, the certification infrastructure was decommissioned and thus there are no TOP-BDIIs and WMS that could be used during the certification process.

4. Secmon is based on the SAM Nagios framework us the monitoring engine, which has been discontinued and is only available for Centos5. Migration to the new ARGO framework requires effort both for the adaptation of the new ARGO Monitoring Engine to the secmon requirements and the for the migration of the secmon probes as the old SAM Worker Node Framework is
absolute.

5. In the past it was decided for simplicity reasons to use the ARGO/Monitoring SU for opening ticket regarding secmon. This has resulted in the misconception that the secmon service was related to the ARGO/Monitoring activity.

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

For SECMON issues:

1. There is no mitigation for this issue. The service will continue to operate but without any new or maintenance developments. The focus of the Secmon team is on the operation of the monitoring engine, integration of new probes when they are available and support through
GGUS.

2. The responsibilities of the previous team members have been transferred to a new person.

3. EGI-CSIRT has developed and proposed a new procedure that will allow for the manual self-testing of the uncertified site and thus central security monitoring for uncertified sites will not be required any more.

4. With the current effort levels there is no activity foreseen for the migration to the ARGO framework.

5. The Security Monitoring SU will be used from now for secmon.

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.)

Most operational security activities will continue as before. IRTF changes will depend on incidents and policy discussions. However, if the FedCloud continues to expend (more users
and more providers), we have to prepare ourselves to handle more incidents.

Still need to progress with some matters concerning contacts relevant to the EGI Federated cloud, as we still do not have means of easily contacting VM endorsers or VM operators in, for example, the case where there is a critical vulnerability concerning operating systems.

For the trust anchor distribution, no changes to the operational service are foreseen. The integration of the IOTA "RCauth.eu" CA in the EGI trust anchor framework may lead to an increase in questions regarding the trust model.

We plan to hold a joint SPG and CSIRT F2F meeting in Amsterdam in December.

Participation and leadership of WISE and IGTF activities will continue.

Many of the team will speak and/or chair sessions at the DI4R conference in Krakow (Sep).

SECMON - No changes to the operational service are foreseen. We will work with the ARGO Monitoring team in order to better understand the requirements for the future migration to the ARGO framework, but until resources are available we will have to continue with the current implementation.