Contribution ID: **39** Type: **not specified**

EGI-CSIRT: Coordinating Operational Security in evolving distributed IT-Infrastructures.

Tuesday, 7 March 2017 15:00 (20 minutes)

Operational Security in Scientific distributed IT-Infrastructures
like EGI is challenging. Existing computation frameworks get further extended,
and new technologies implemented.

In this evolving environment new policies have to be developed, and existing
policies and procedures have constantly to be extended to meet new requirements.

To efficiently enforce new policies, the security monitoring infrastructure has
to be further developed to cover all elements of the evolving infrastructure.
Finally the incident response (ir) tool set has to be extended to be able to
efficiently handle security incidents affecting new technologies.

In this presentation we will discuss EGI-CSIRTs way towards extending its
portfolio to also provide all aspects of operational security in a Cloud environment.
This covers the developments around the Virtual Machine Endorsement Policy and
the related technical aspects towards a trustworthy set of Virtual Machine
Images (VMI) offered to the user community through an Application-DataBase.

VMIs with vulnerable configurations were already involved in incidents handled by
EGI-CSIRTs Incident Response Task Force (IRTF). Here it got apparent that the
existing procedures and tools, which were successfully applied in IR in EGI,
exposed deficiencies when applied to the FedCloud services.
This triggered the development of a central User- and Virtual Machine-Management
for frameworks deployed in EGI-FedCloud.
The status of these tools will be demonstrated and the integration with the
existing IR tools discussed.

In EGI the policies and procedures are put to a test in so called Security
Service Challenges (SSCs) to check if they indeed help in security operations
to prevent and respond to incidents.
An SSC addressing EGI-FedCloud interfaces and IR procedures will be described.

Primary authors: Dr KOURIL, Daniel (CESNET); Dr GABRIEL, Sven (Nikhef/EGI); Mr BRILLAULT, Vincent (CERN)

Presenters: Dr GABRIEL, Sven (Nikhef/EGI); Mr BRILLAULT, Vincent (CERN)

Session Classification: Network, Security, Infrastructure & Operations I

Track Classification: Networking, Security, Infrastructure & Operations