Contribution ID: **67** Type: **Oral Presentation**

EGI-CSIRT: Organising Operational Security in evolving distributed IT-Infrastructures

Thursday, 17 March 2016 16:00 (30 minutes)

Operational Security in Scientific distributed IT-Infrastructures like EGI are challenging. Existing computation frameworks are further extended, and new technologies implemented. In this evolving environment new policies have to be developed, and existing policies and procedures have to be extended to meet the new requirements. These policies and procedures are then put to a test in so called Security Service Challenges (SSCs).
To efficiently enforce new policies, the security monitoring infrastructure has to be developed to cover all elements of the infrastructure. Finally the incident response tool set has to be extended to ab able to efficiently handle security incidents involving 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 involved in incidents handled by the EGI-CSIRTs Incident Response Task Force (IRTF). This triggered the extension of the existing incident response tool set to allow for central User- and Virtual Machine-Management frameworks, needed to efficiently respond to threads exposed by compromised systems in EGI-FedCloud.

Primary author: Mr GABRIEL, Sven (Nikhef)

Presenter: Mr GABRIEL, Sven (Nikhef)

Session Classification: Networking, Security, Infrastructure & Operations Session V

Track Classification: Networking, Security, Infrastructure & Operations