Contribution ID: **69** Type: **Oral Presentation**

Assessment of the incident response processes in a Distributed Infrastructure

Tuesday, 2 April 2019 16:30 (30 minutes)

EGI CSIRT provides operational security to distributed compute infrastructures coordinated by EGI. One of EGI CSIRTs activities is to assess the overall incident response capabilities, which is done through security exercises, so called Security Service Challenges (SSCs).
Operational security in an agile environment with different job management systems, logging information at different locations and entities coordination of the involved security teams is key.

The used services need to provide sufficient traceability of user actions as well as interfaces to the systems that offer methods needed to contain an incident, i.e. suspending of credentials found in activities violating approved security policies.

In an assessment of the overall incident response capabilities one of the core aspects will be the junctions between the acting security teams, each having a different view on the situation and different tools available to contain the incident.

To be able to run Security Service Challenges (SSCs) targeting multiple Resource Centres (RCs) and Workload Management Systems (WMS) a framework, the SSC-Monitor, was developed, that allows for central management of the malicious activities as well as for recording and evaluating the expected actions of the participating CSIRTs. This SSC-Monitor was already used for earlier SSCs. While large parts of this framework remains constant several adoptions are needed to implement the Virtual Organisations WMS. Also to be able to measure the incident response of the participants various metrics have to be developed and made available to the SSC-Monitor, and in order to realistically hide the malicious activities, alternative methods for getting the payload to the compute nodes had to be researched and implemented into the SSC-Monitor. Details are presented in separate contribution to this conference.

In the SSC presented here we focused on the WMS Dirac developed and used by the LHCB VO. Incidents involving a VOs WMS require actions and information flow from/to the VOs security team, the RCs security teams and, eventually, additional entities providing authentication frameworks. The information flow and the orchestrated incident response activities are coordinated by EGI CSIRTs Incident Response Task Force (IRTF).

To assess the readiness of the above mentioned security teams, EGI CSIRT together with the VO LHCB created a realistic incident scenario, where valid user credentials are used to submit jobs to the infrastructure using LHCBs workload management system DIRAC as well as using generic services available for job submission directly to the sites.

In this presentation we will show the detailed incident scenario created by the SSC-Monitor, the expected actions described in the incident response procedures as well as the efficiency of the actions described in the developed metrics.

Primary authors: Dr HAEN, Christophe (CERN); Dr GABRIEL, Sven (Nikhef/EGI); Mr BRILLAULT, Vincent (CERN/EGI)

Presenter: Dr GABRIEL, Sven (Nikhef/EGI)

Session Classification: Networking, Security, Infrastructure & Operations

Track Classification: Network, Security, Infrastructure & Operations