Contribution ID: **131** Type: **Training**

Security Incident Management in the EOSC era Part-2

Thursday, 11 October 2018 14:30 (1h 30m)

The security training proposed here would be split into two sessions, focusing on different areas of incident handling. An important area that will be highlighted is the close collaboration of experts necessary for the successful resolution of a security incident in the EOSC era

The first session targets the more technically oriented attendees. Here, after an introduction to forensics, the participants will have to analyse images provided by a security team of a FedCloud site. The results of the investigations will be used as input for the second session, where the case will be handled within a role-play involving the various service providers active in the EOSC-Hub project, including identity providers, SIRTFI, the service catalogue, and the infrastructures coordinated by EGI and EUDat.

The goals of this training are twofold. Firstly, the collaboration of project members with a managerial background and those with a technical background will be explored. The second goal is to examine the existing set of policies and procedures to challenge them and identify possible issues. It is hoped that this will help to prioritize the security related activities within the EOSC-hub project.

Summary

Starting from the security incident report, summarizing the findings of the forensic investigations in Session-1, we will handle a high profile incident.
The incident will be coordinated by the Incident Response Task Force, and the discussed incident response activities will be based on the existing set of policies and procedures.
In course of the role-play we will also trigger the higher level aspects of incident handling, like the escalation to legal, press, and management of the infrastructures and service providers active in EOSC-Hub.

Type of abstract

Training Session

Primary authors: KOURIL, Daniel (CESNET); Dr CROOKS, David (UG); GROEP, David (NIKHEF); KELSEY, David (STFC); Dr GABRIEL, Sven (NIKHEF); KAILA, Urpo (CSC); BRILLAULT, Vincent (CERN)

Presenters: KOURIL, Daniel (CESNET); Dr CROOKS, David (UG); GROEP, David (NIKHEF); Dr GABRIEL, Sven (NIKHEF); KAILA, Urpo (CSC); BRILLAULT, Vincent (CERN)

Session Classification: Training: Security Incident Management