CSIRT IRTF

Incident Response Task Force

Objective

Handle day to day operational security issues and coordinate Computer-Security-Incident-Response across the EGI infrastructure.

Tasks

- Swift response to any reported computer security incident affecting EGI infrastructure
- Security Incident Management
    - Existing communication channel (mail list/security wiki) migration
    - New communication channel (if needed) setup
    - Incident response tools development, evaluation and adaptation
    - Incident handling procedures update/maintenance
- Establish additional operational and/or escalation procedures when required
    - a procedure to suspend a site from the EGI infrastructure
    - a procedure and agreed criteria to ban (blacklist) a user, a group of users and/or a VO
- Maintain and extend open source intelligence and information exchange with trusted partners
    - Gather information about current cyber attack and threats
    - Derive monitoring rules applicable to EGI

Coordinator

- Pinja Koskinen from CERN