Security Incident Response Procedure for Inter-Federation

How can we coordinate a response to a security incident affecting multiple national identity federations, research communities, campuses and online service providers? Who has responsibility for resolving an incident? Can we maintain confidentiality? Are the relevant capabilities for incident recovery available within the inter-federation and are these capabilities available to every participant?

This is one of the challenges being analysed by the AARC Project, https://aarc-project.eu, and is an essential building block for a reliable authentication and authorisation infrastructure. This poster presents the AARC proposal for building a sustainable security incident response capability for eduGAIN, the global inter-federation for research and education, in line with the existing trust model.

The proposal builds upon the requirements of Sirtfi, the Security Incident Response Trust Framework for Federated Identity, which has been widely accepted by the global community of identity federations over the past year. This framework is used to hold all participants to a common set of behaviours and guarantee the trustworthy exchange of information.

Primary author: Ms SHORT, Hannah (CERN)

Co-author: WARTEL, Romain (CERN)

Presenter: Ms SHORT, Hannah (CERN)