Generic Security Incident Response Procedure

This document provides homogeneous, scalable security incident response procedures to ease collaboration in the event of a security incident impacting multiple, distinct organisations. This capability has been identified by Research Communities as a prerequisite for the widespread adoption of federated identity management. To support the procedures, this document contains background information on the concepts and processes required for security incident response in a federated environment.

The Sirtfi framework will form the basis of such a procedure; the Sirtfi mechanism and consultation model are (briefly) recapitulated in this document, and the same model will be used to obtain a global rough consensus on security incident response for federated incidents.

The document contains a detailed proposal for coordinated response: this model should be considered as the basis for discussion in the REFEDS Sirtfi group. It is based on experience with handling actual incidents, and as such contains detailed recommendations. Yet it is also meant to be open for discussion as the global community participates in the endeavour.

AARC Information Document with the Guide to the Response Procedure - AARC-I051

Following the second federated incident response challenge, the processes used then (as well as the requisite steps to be well-prepared for incident response) have been collected in an AARC Information Document: AARC-I051 Although short of a formal Guideline (since the process and procedures are under continuous development in the REFEDS Sirtfi Working Group), it clearly lays out the necessary steps to prepare for, act on, and report and share information about federated security incidents.

Use the proposed "Generic Procedures" now if you are faced with an incident extending beyond just your own organisation:

- I051: Guide to Federated Security Incident Response for Research Collaboration (MSWord, docx)
- I051: Guide to Federated Security Incident Response for Research Collaboration (PDF)

Previous Document versions:

- Final "D3.2" version: https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf
- DNA3.2 Security Incident Response Procedure v0.2.pdf (or in MS Word XML format)
- DNA3.2 Security Incident Response Procedure v0.1-DG.docx
- DNA3.2 Security Incident Response Procedure v0.1.docx