Sirtfi WG google folder:

https://drive.google.com/drive/folders/13EhgPxzLy4U6FMP_cVDaIbqju40hOhUR

Current/Recent Tasks

Who	What	When	Status
Romain	Add Act-Inform diagram to the eduGAIN security wiki when it gets created		

Older tasks are at the bottom of running Sirtfi call notes document.

March 11, 2021

Attending: Alan B, Hannah, DaveK, Romain, DavidG, Pal, DavidC, Tom B, Uros S, Sven G, Shannon R, Mario R, Daniela P, Pål A, Brett B

Regrets:

Agenda:

1. Question from the field:
    a. What details should an SP send to an IdP when they detect a potentially compromised account
    b. Does Sirtfi ask the SP to ensure that their infrastructure enables them to identify all of the services behind their SP (which proxies their several services)?
2. Complete/refine logistical ideas raised earlier (see notes from Feb 11 meeting below)
3. AOB

Further logistics bullets upon reviewing those from Feb 11:

- Use eduGAIN steering as means to communicate with FOs
- Yes, ask FOs first
- But first thing is to talk with Nicole for guidance
- Also send to e-infra operators, ie, to get RPs behind proxies. Use FIM4R and AEGIS lists.
- Message to FOs includes “please reply by $date, after which we'll proceed unless told otherwise”.
- Message to FOs: we want to reach all of your members.

Add a question on the survey asking IdP or SP or both or proxy, and write-in your federation(s). Both optional. Or better, address this in intro to survey: if you speak for multiple, have your answers express the union of your experiences across them.

Tom AIs:

1. Amend survey
2. Send trial survey to sirtfi list for tire-kicking
3. Speak with Nicole about logistics

The WG also spoke about the question in agenda item #1, basically to agree with what Tom told the SP operator (as his personal opinion):

a. Their choice of technical data to send (Response ID, IssueInstant, Issuer) is appropriate: sufficient for an IdP to link to a user account and contains no personally identifiable information. We also agreed that any further info that might be relevant for IR, eg, IP addresses, could wait for follow up communication between those parties.
b. Sirtfi doesn't and shouldn't weigh in an Organisation's decisions about how to architect their service or what info to propagate through it. It is sufficient, for the SP to be able to tie an IdP login session with a potential security incident. We also noted that it naturally behooves the Organisation to try to determine the entire extent of the breach within their systems, but Sirtfi does not obligate them to do so.