Sirtfi WG google folder:

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

Task List

Who	**What**	**When**	**Status**
Nicole	Collect several fed security plans.	Done	https://wiki.refeds.org/display/GROUPS/Federation+Incident+Response+Plans Notes: FOs don't sign up for Sirtfi - do we need a template / criteria for involving them in incident response? Is the AARC doc the right set of template things we want them to do? https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf
Nicole	Check with WAYF on how they do their incident response - is it like other hub and spokes?	Feb 28, Done	A: Surfnet style model, no english documentation, playing a heavy role in managing incidents
Shannon	Report on REN-ISAC information sharing guidelines (2.d)	Done	REN-ISAC ISP Public, Limited, Privileged, Restricted Use information are of interest
Romain	Gather IR plans from some e-infrastructures	Feb 6	
Hannah,	Update templates with experience from	Done	Initial set in in IR

Romain	table tops. Hannah and others have already outlined these in another report. Place results in subfolder of the sirtfi google folder, for now.		Templates subfolder
Laura	2.c Incident response team communication: Outline a set of requirements for a communications tool (to help with tool selection)	Done	Held a session during the TIIME meeting where the group provided a set of tool requirements and some suggestions of tools. NOTES
Mario	Brief Geant 4-3 IR meeting attendees on Laura's task, maybe arrange Laura's remote participation		I mentioned Laura's work to Daniel Kouril from GN4-3 - will need to include also others in the loop. Will get back to Laura about this.
Shannon, with input from Doug Pearson	Bullets that describe how REN sharing agreement doc should be transformed for (1) federated IR management team context, and (2) broader notification, sharing, or publishing		"user stories", problem description. Pending discussion with Doug.
Scott	Contact InCommon to see if keeping security contact information fresh could become part of baseline requirements, and use InCommon to investigate and draw out both the policy and the technical implementation. Keep Nicole, Laura, Mario, and Pål in loop. Mary-Catherine Martinez <mc.martinez@innosoft.ca> is Community Trust and Assurance Board chair.	Done. Initial email sent to Mary-Catherine Martinez	June 5 2019 Scott met with InC's Community Trust and Assurance Board about partnering with them to investigate doing this. Positive response from CTAB. Small WG forming to dig in.
Nicole	Prepare to operate sirtfi.org website - eg, make it a blank wordpress site	Done for now	Registered by Scott, discussed transferring
Nicole	FOs don't sign up for Sirtfi - create a template / criteria for involving them in incident response (i.e. get FOs to declare what they are doing and start actively monitoring this). Also encompasses	In Progress	Raised at Steering Committee, small WG created.

	defining what FOs should be doing during incidents.		
Laura + conscripts	Distill essential requirements from TIIME tool talk (Laura’s item above) and identify one or two possible solutions.	Done	Draft tool req doc | federation survey | REFEDS discussion?
TBA (Nicole?)	Promote “Transits” CSIRT training to (some) FOs. Possibly compress that 3 day event into 1.5 days or so. Who should take this earlier? eduGAIN support? Some specific FOs? (Also see what material is applicable)	Done	Proposed TRANSITS in 90 minutes at REFEDS at TechEx and get feedback there on usefulness.
Tom	Create user stories doc in Sirtfi WG folder, add Shannon’s, and WG members add to it as stories occur	Done	Doc created.
Tom	Clean up WG task list on the wiki	Mar 28	Done
*	Add user stories to the doc.		
Alan, Hannah	First stab at thinking through Per Role docs. Comments are welcome!	Done	Draft IR roles doc started. It’s really interesting, everyone take a look!
Tom	Draft outline of IR in R&E Feds	May 9	Initial draft outline complete
Hannah	Add a User Story about wider notification of lessons learned & recommendations based on the incident experience.	Apr 11	Done
Hannah	Updates to IR templates as discussed on March 28	Done	
TBD	When IR Roles doc is somewhat baked, check to see if IR Templates contains a template for each function in IR Roles.		
Nicole	Add use cases to the User Stories as appropriate to describe the types of scenarios/obstacles encountered in the recent incident discussed on the Apr 25 WG call.		Organisations removed information from the public domain.

	Update: maybe still interesting from a process perspective even if details can’t be public.		
Alan, Hannah	Continue with IR roles and include in Handbook		
Tom + Romain + ??	Continue work on IR Handbook		
Uros	Start a doc on the Sirtfi + eduTeams question, and get Christos to explain it to us.	Done	Doc
Nicole	Peruse NGI Trust funded projects to identify any that may be relevant for Sirtfi.		
Romain	Draw picture of hierarchical structure of large scale (federated) IR, including processes to join branches and leaves to the hierarchy.		
Hannah, Christos, Alan	Brainstorm good, bad, and ugly potential resolutions to the question that Uros and Christos brought to the WG, as described in the August 1 2019 notes below and in Proxy asserting Sirtfi as an IdP.	Aug 15	

August 15, 2019

Attending: Pål, Hannah, Uros, Romain, Laura

Regrets: Tom B

Agenda:

1. Review open tasks
    a. No progress
2. Try to determine the position the WG should take for the use case discussed last time.
    a. Proxy asserting Sirtfi as an IdP
    b. Notes following previous discussion
    c. Notes from today

i. Romain: asserting Sirtfi compliance is within your own domain, you cannot assert it for anything outside that. In general these sound like operational security issues, not Sirtfi compliance issues.

ii. Laura: an unwritten expectation of proactive notification (planned in v2 of Sirtfi) and concern of broken trust in the case of proxies. Expectation of global community protection.

iii. Examples

1. Real life examples, e.g. IdP as a service, eduTEAMS
2. Hypothetical example 1: EGI Fed Cloud allows any eduGAIN user from a Sirfti compliant IdP to create VMs. eduTEAMS is listed as a Sirti compliant IdP in eduGAIN, because it has an additional process for confirming emails and general satisfies the Sirtfi framework. A user with an anonymous ID may be able to use eduTEAMS to create VMs in EGI Fed Cloud.
3. Hypothetical example 2: You use a SP with a google account that blocks you, then you access it again through eduTEAMS and are able (actually this is not to do with Sirtfi...)

iv. We are maybe trying to roll up Assurance aspects into Sirtfi, which is not its job. However, there is a spirit of Sirtfi and many expectations regarding willingness to participate in a collaborative process for incident response.

v. General feeling that from a pure Sirtfi level, the proxy should be able to assert Sirtfi if it genuinely supports the framework within its domain of influence. There are multiple other issues with the idea of re-inserting a proxy IdP into eduGAIN, including propagation of assurance and account linking or whitewashing - these are not a problem with Sirtfi.

3. Interesting aside, how would proactive notification work? Should escalate to eduGAIN security team who will help contain the incident :) There shouldn’t be a problem with sharing these details under GDPR, legitimate interest to protect the infrastructure. Not being able to play an active role in checking account compromise, as an SP, doesn’t help trust.
4. Actions:

a. Propose a call on proactive compromise notification, in collaboration with the eduGAIN security team

b. Suggestions for a future meeting:

i. Sirtfi adoption, how is it going

ii. Are the value statements for different participants clear and compelling and meeting expectations of those participants

iii. Revisit the original intent of Sirtfi - how are we doing? Should it officially be revised?

iv. Should there be a campaign among key SPs to require Sirtfi to drive adoption?

c. Hannah create statistics on where Sirtfi compliant entities are coming from

5. AOB