,Sirtfi WG google folder:

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

Current Task List

Who	What	When	Status
Romain	Gather IR plans from some e-infrastructures	Feb 6	
Mario	Brief Geant 4-3 IR meeting attendees on Laura's task, maybe arrange Laura's remote participation	Closed	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. Task overtaken by events.
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 defining what FOs should be doing during incidents.	In Progress	Raised at Steering Committee, small WG created.
TBD	When IR Roles doc is somewhat baked, check to see if IR Templates contains a template for each function in IR Roles.	Closed	
Alan, Hannah	Continue with IR roles and include in Handbook	Closed	
Tom + Romain + ??	Continue work on IR Handbook	Closed	
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.	Done	pptx: https://drive.google.com/file/d/1X8rqXorYgO_ihqCepW6n2Z2PXgn24WVY/view?usp=sharing PDF: https://drive.google.com/file/d/1osCQeFVQyGY4LgnKUk-ilqvqQPppHOhp/view?usp=sharing
Christos	Propose a REFEDS 2020 Work plan item focused on understanding and potentially "regulating" proxy IdPs.		
Laura	Propose an ACAMP session on stakeholder expectations of Sirtfi.	In progress	
Hannah	Sirtfi 'ad' for eduGAIN website (aimed at Fed Ops). All to provide comments. https://docs.google.com/document/d/1trIFfKHC9lTlFMW0tI25r9q8KL4LLHmuhtHzV1Z_4x4/edit#	In progress	
Hannah	Ask Davide whether security contacts for Fed Ops exist	Done	Yes (WIP) https://technical.edugain.org/status
David G, Uros	Improve sharing procedures in AARC DNA3.2 paper by folding in experience from EGI.		

November 21, 2019

Attending: Romain, Tom, DaveK, Pål, Sven Gabriel, David G, Shannon R, Daniel Kouril, Laura

Regrets: Alan B, Uros

Agenda:

1. Task review

2. Sirtfi at TechEx/FIM4R
3. Update on prospects for new table top exercises.
   (Make mention of the current OSG-EGI security drill)
4. Status of Sirtfi+ Registry incubation project.
5. Main business: depiction of large scale IR (Romain)
6. AOB

There will be discussion at the upcoming FIM4R meeting at TechEx about notifying downstream entities of compromised accounts. Like we plan for Sirtfi v2 in Phase 3 of our work plan, but applicable more broadly than just R&E federation members, Sirtfi's current scope.

No news about table top exercises.

The Sirtfi+ Registry incubation project has been extended another 6 months.

Romain made his presentation (PPTX and PDF forms are available, the PPTX performs substantive animation). TLP sharing details; central coordination, but that's all relative - each domain has its own procedures and tools, and conveys info according to TLP using their own processes. Romain also spoke about a particular account compromise that illustrated how these large scale IR response procedures start to happen.

Laura noted that TLP white/green info is shared only in accord with federation/e-infra security policy, so it is important to ensure that those policies include appropriate sharing. Since that solution involves many pieces, would it be simpler to have a central website on which white/green info can be published. DavidG supposes the Geant wiki can be such a place, which includes federated access. Parties lacking institutional federated identities can get another for this access.

Paål asks do we lack something essential to enable the flows that Romain showed? Answer: no, we're good.

Tom asked Romain about centralised process to identify and notify about compromised accounts (as Romain described in his example above) versus decentralised process as envisioned for Sirtfi v2. Basically, both are needed, especially since each will be flawed: centralised will miss many things, and many organisations will fail to fulfill their obligations in a decentralised model.