Sirtfi WG google folder:

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

Task List

Who	What	When	Status
Nicole	Collect several fed security plans.	closed	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	Request sent. Response pending.
Shannon	Report on REN-ISAC information sharing guidelines (2.d)	Jan 31	REN-ISAC ISP Public, Limited, Privileged, Restricted Use information are of interest
Romain	Gather IR plans from some e-infrastructures	Feb 6	
Hannah, Romain	Update templates with experience from table tops. Hannah and others have already outlined these in another report. Place		

	results in subfolder of the sirtfi google folder, for now.		
Laura	2.c Incident response team communication: Outline a set of requirements for a communications tool (to help with tool selection)	Feb 28	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 people of 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	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		
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.		
Nicole	Prepare to operate sirtfi.org website - eg, make it a blank wordpress site		Registered by Scott, discussed transferring
Nicole	FOs don't sign up for Sirtfi - create a template / criteria for involving them in incident response		
Laura + conscripts	Distill essential requirements from TIIME tool talk (Laura's item above) and identify one or two possible solutions		
TBA	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?		

February 28, 2019

Attending: Tom, Laura Paglione, Nicole, DavidG, Shannon Roddy, Romain

Regrets: Scott, Pål, Uros

Proposed agenda:

1. Tom update group on discussion with Doug Pearson and Kim Milford of REN-ISAC
    a. Doug will reach out to Shannon to offer thoughts on his task (above), especially about information sharing (sending and receiving) outside of the context of managing an incident.
    b. Consider identifying a responsible party for managing in-response communications, for example, slack channels, to ensure efficient and appropriate use of those.
2. Task review
3. New tasks
4. What deadline should we set ourselves for initial completion of a federated security incident response paper laying out roles, responsibilities, tools, procedures, etc?
5. Other business

Romain: GN 4-3 (edugain support) working already on incident response. He and David to do their best to maintain alignment with Sirtfi WG.

Develop guidelines for fed ops to support fed IR, maybe further. Will we have enough time? Is the list that AARC defined enough and how does a Federation Operator sign up to following these bullets?

- Follow the [IR] requirements described by Sirtfi, and [OS], [TR] and [PR] as applicable.
- Provide a security contact point (e.g. security@federation.org) available to all federation participants,federation operators, other federations and external organisations.
- Define communication channels to be used for security incident response by federation participants.
- Appoint a Federation Security Incident Response Coordinator when notified about a suspected security incident. (This role may be played by a federation participant or external entity, such as a Research Community or e-Infrastructure CSIRT, as appropriate).
- Ensure a unique identifier is assigned for each security incident.

- Provide or source technical expertise necessary to assist federation participants (forensics, technical investigation, log analysis, etc.)

Keep essential docs in multiple languages.

NB: We may need to evangelize funders to increase funding to FOs to enable IR, hence basic trust in their part of interfederation.

WG agreed that we'd set REFEDS at TNC19 as a deadline for mapping out, eg, bullet form, all of the "guts" that will go into the WG's FSIR paper.