Sirtfi WG google folder:

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

Current Task List

Who	What	When	Status
Tom	Ready the IR Handbook for Consultation and write Nicole about it.		June 30, 2020: Done.
David G	Ask AEGIS members to check/confirm that they have an open channel to their federation operators to ask about readiness for incident response.	Jun 4, 2020	
Tom	Ask eduGAIN security team to update the WG periodically on what's been going on.	July 16, 2020	
Tom	Update work plan in the wiki	July 16, 2020	

July 16, 2020

Attending: Tom, DavidC, Shannon Roddy, Dave K, Sven G, Hannah, Lino K

Regrets: Alan B, Mario R

Agenda:

1. Next steps for the WG (refer to overall plan in the Sirtfi wiki)
    a. Does the WG believe that the IR Handbook sufficiently fulfills its deliverable of "Define incident response procedures for federations, including communication templates, and support the community in their adoption"?
    b. Your thoughts about the next task the WG should undertake
    c. Change/add/delete plan items?
    d. Seek consensus on the next task for the WG
    e. Initial planning for doing that task
2. AOB

Ideas:
Work with eduGAIN Security Team to build out some templates.

When do we know we're done with: "Test incident response process and use of security contact metadata in simulated activity." ?

We have already worked towards "Establish communication channels for security information exchange and incident report sharing." and have decided that it is not doable or worthwhile. Mark as done; note this conclusion in the wiki.

We've done lots already towards "Promulgate educational and communication materials to help R&E federations to promote and support Sirtfi public v1.0 adoption.", and we're doing more in connection with the eduGAIN IR Handbook. Mark as done.

The task "Implement processes by which to maintain and broadcast security contact information and Sirtfi trust framework adherence, outside standard federation metadata publication mechanisms." has "just flopped". Much was done towards this end, but it's done.

Re Phase 3 work items:

Testing freshness of security contact info.

Re LIGO, ask Scott about the Sirtfi+ Registry, if it's still needed.

Add "maintain your security contact in federation metadata" as a required specification in Sirtfi v2.

Add item regarding on-going responsiveness checks.

Re "Develop tools to help IdPs identify accounts that have been used to access specified SPs.", is this too far in the weeds? Sirtfi v1 already requires keeping logs, and admins already use grep or elastic search to parse logs. Strike this one, it isn't realistic.

Consider adding to Sirtfi v2: adequate TLS implementation on federated entities. Or perhaps a work item in itself, to have global monitoring of endpoint security.

We really don't have data about the effectiveness of v1, so might be too soon to produce v2.

[Tom]: Ask eduGAIN security team to update the WG periodically on what's been going on.

[Tom]: Update work plan in the Sirtfi wiki.