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 4, 2020	Consultation period ends Sep 11.
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, and suggest they draw on Hannah's templates.	July 16, 2020	July 16, 2020: Done.
Tom	Update work plan in the wiki	July 16, 2020	July 16, 2020: Done
Tom	Ask Scott K about LIGO and the Sirtfi+ Registry	July 16, 2020	July 17, 2020: Done. LIGO's need was to get some IdPs in the Indian federation shown as sirtfi compliant, but LIGO-India decided to operate its own IdP instead.
Alan B	Read IETF Security Events docs and discuss impressions at next WG meeting (Aug 13, 2020)	July 30, 2020	
Tom	Create initial draft survey about Sirtfi v1	July 20, 2020	
Tom	Send email to REFEDS list on ~Aug 11, about 1 month before Consultation period	July 30, 2020	pending

	closes, asking Fed Ops especially to look at the IR Handbook under Consultation.		
Tom	Ask Pål about the use of MISP across a national federation.	Aug 13 2020	

August 13, 2020

Attending: Dave K, David C, Uros S, Alan B, Tom B, Shannon R, Hannah S

Regrets: Sven, Romain

Agenda:

1. Review tasks
2. [Alan B] Initial thoughts about using IETF Security Events in support of federated incident response
3. Seek consensus on the next task for the WG
    a. If it’s the survey, proceed with rest of the agenda below
    b. Else initial planning for the next task
4. Survey focus
    a. Objectives
        i. Learn from those who’ve asserted Sirtfi
        ii. Learn why some haven’t done so, and coincidentally educate about Sirtfi
    b. Recipients
        i. Security contacts at Sirtfi entities only?
            1. If so, send directly or go through FOs?
        ii. Admin/tech contacts for each entity (limiting 1 for each address)?
        iii. Ask FOs to send it however they will?
    c. Fed Ops engagement & coordination
        i. Use REFEDS list or FO contacts?
        ii. Consultation on the survey instrument before asking FOs to send?
        iii. Per-federation timing?
        iv. Per-federation tuning of questions (fed-specific questions, context, language)?
5. AOB

Discussion of #2

RFC 8417. SET = Security event token. Notify about email address reassignment; similar to eppn reassignment. HTTP poll/push drafts describe how to move SETs around, eg, in a message bus. Not specified: encryption, etc, metadata about whether/how to encapsulate SETs. Existing fed metadata can be used for that. SETs can contain PII, possible GDPR issues. The main questions concern architecture and policy for sending SETs around federation, together with development and maintenance of supporting technology.

EGI considered using SETs for account (DN) suspension (in place of or in parallel to ARGUS). Since they already have something that works, they haven't taken it further. Maybe for interfederation use cases.

Possible federation use cases:

IdP notify concerned SPs of:

- Eppn or email has been reassigned
- User account expired
- User account locked

SP notify concerned IdP of:

- AUP violation by user account

Real issue is the architecture of the messaging system that all IdPs can publish to and all SPs can subscribe to. Maybe per-federation aggregators. Also requires substantial automation associated with each federated entity. Passing SETs through a proxied ecosystem is an additional dimension.

IdPs and SPs can’t query. Eg, user X just logged in to SP Y, which wants to ask user X’s IdP if their account is still active and assigned to the same person. That isn’t supported. But SP Y can monitor SETs originating from IdPs that present users in SP Y’s user database and react appropriately to SETs concerning its users.

There is no notion of audience in a SET, but architecture might use various different messaging queues, and the publisher sends to appropriate queue(s). Or suitable use of encryption to limit who can read a given SET.

Is the technical means by which to share security information a central problem for us? Is it an equivalent architectural problem to consider using MISP/CES as that global platform? Perhaps, modulo strengths and weaknesses of each. MISP/CES translation is being looked into by Liviu & Vincent from CERN. The main benefits lie in having some system that enables automated rather than manual response to some events, and in having an improved perspective of the scale of such events.

Implementation of a SET-based layer on top of global R&E federation is a big leap, especially considering the complex policy, operational, and technological requirements.

Is there an R&E Fed using MISP to send around security events? Sweden, Denmark, one of the nordics?
[Tom] ask Pål.

The WG decided to proceed with the Sirtfi v1 adoption survey as its next task. The WG also decided not to remove the item related to using SETs (or MISP perhaps) from its work plan, at least not yet. We'll try to learn what that nordic federation has been doing before returning to this item.