## 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<br><br>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) | Done | 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 | Done | Initial set in in IR Templates subfolder |

| | | | |
|---|---|---|---|
| | 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) | 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.<br><br>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 | | |
| Laura + conscripts | Distill essential requirements from TIIME tool talk (Laura's item above) and identify one or two possible solutions. | | 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? | | |
| 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 | | 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 | | All but 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 discuss on the Apr 25 WG call. | | |

## June 6, 2019

Attending: Scott, Tom, Romain, Brook, Laura, Shannon, Hanna, David G, Alan, Uros

Regrets: Pål

Agenda:

1. Review open tasks

   Scott recounted good engagement with InCommon's Community Trust and Assurance Board, agreement to take this up especially as they appear poised to tee up a security-focused next step for Baseline Expectations. Several members volunteered to join a focused team to work on this. Scott will help put that together.

   David G mentioned WISE and SIG-ISM efforts parallel to what Scott discussed with InCommon. [https://wiki.geant.org/display/WISE/SCCC-JWG]. Scott and all agreed to try to liaise between these related efforts, avoid needless duplication or differences.

2. Next steps on tools
   a. IR in R&E Feds section provides high level description of purpose to be served by a tool
   b. Do we agree this is the immediate need for a tool, ie, so that
      i. the IR handbook can be completed
      ii. we can concretely articulate the obligation of the "IR team support org" posited in the handbook and hence get a commitment from a real org to provide that function
   c. Record here other really good things that tools might do that come up in the above discussion but are not the immediate need:
      i.
   d. If we concur on the immediate need and its description in the handbook
      i. Will its selection be controversial?
      ii. Do we want to gather input as part of the selection process?
      iii. Does the draft survey do a good job of that?

   Most of the hour was spent in discussion of the above with little concrete progress apart from clarifying some of the different perspectives that WG members have over what they hope to see come from our efforts. Somewhat rehashing the discussion from the previous WG meeting, these points emerged:

   - Some view the central problem to be addressed as best preparing things so that an IR team can identify the nature and extent of an intrusion as soon as possible, and determine steps needed to respond.
   - Others view the central problem to be outward communication to affected and potentially affected entity operators so that they can be aware of what's happening and allocate their time better for having this information.
   - Some are concerned that tools and processes already established in federation represent latent resistance to establishing something different that may be employed in federated IR, though it was acknowledged that this does not mean we should do nothing to enable better federated IR.

- The above lack of clarity and consensus also explains why there was no clear impetus for doing any sort of survey, as was considered at the last WG meeting.

3. SIRTFI WG update at REFEDS40
    a. Tom has 20 minute slot. Suggested split:
        i. ~5 minutes: update on work plan and where we're at, maybe outline of IR handbook
        ii. ~15 minutes: discuss/in-room poll on tool-related matters
4. Other business

    None.