May 24, 2018

Attending: Tom, Alan, Romain, Shannon, Hannah, Pål

Proposed agenda:

1. Agenda bash
2. TNC18 planning
   - a. Who’s going?
   - b. Material for the REFEDS WG update
     - i. What we’re up to
     - ii. Tabletop exercise report out
     - iii. Breakdown of security contact types (grep some metadata)
     - iv. Registry ‘thingie’ (https://docs.google.com/document/d/1wh2SQU62zDRwlJLPFgwxmRnIq7IiVgPf76XI97Hzt80/edit?usp=sharing) models - vote or other feedback?
     - v. “FSIR” most pragmatic thing ever!
   - c. Opportunities. Who will be there that someone should chat up?
     - i. Communication & info sharing channels for FSIR and their operation
       1. Hannah
     - ii. Anyone at GÉANT/elsewhere working independently on FSIR procedures that we should incorporate into this WG?
       1. CLAW (Alf, Charlie ?) - Hannah
     - iii. GÉANT thinking about nature of central coordinating role they’re up for
       1. Hannah
     - iv. Solicit thinking on Sirtfi adoption and what the Registry ‘thingie’ should do and consist of
       1. Alan
   - d. Managing expectations
     - i. When is the FSIR Procedures paper expected?
     - ii. What, basically, is our aim for the Sirtfi Registry thingie, and when will those requirements be finished?
3. “Federated Security Incident Response Procedure” paper
   - a. Any reactions upon (re-)reading the AARC version?
     - i. Specific thing to change/add, feedback from AARC
       1. Which contact to use? (all)
       2. How to contact them? (To, not Cc or Bcc)
       3. Include templates with expected questions to ask during an incident
   - b. By what date should we aim to have the REFEDS version ready?
     - i. What starves or veers for lack of it?

     In Autumn AARC would like to test these procedures with another tabletop. Can be an initially complete draft, short of a product of consultation.

c. Work streams:

i. Connecting with related communities/orgs

1. FYI - Meeting this afternoon with InCommon, Trusted Introducer, and REN-ISAC.

ii. Figure out how to quickly add incident responders and share sensitive info during incident management

1. Perhaps related: how do we share sensitive info *before* an incident has happened? Eg, Robot.

iii. Figure out who should perform on-going checks of which sets of security contacts - *and what to do if a check fails*.

iv. Writing the paper itself

d. Process?

4. Else

a. Awareness on possible federated incidents and how people are connected. Some starter material potentially at https://hshort.web.cern.ch/presentations/20170927_DeIC_Sirtfi.pdf

b. Seems to be significant problems with actually using Sirtfi contacts (adoption, ease of use)