Sirtfi WG google folder:

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

May 7, 2020

Attending: Tom, Dave K, David Crooks, Pål, Romain, Hannah, Alan B, Sven, Marina

Regrets: Uros

Agenda:

1. Complete review of eduGAIN Security Incident Response Handbook, ie, review Doc 3.
    a. Are communication templates needed? If so, should they be referenced in the IR Handbook?
2. IR Handbook implementation support
    a. How should this WG and others help prepare everyone to play their IR roles?
    b. Is any tooling needed to support AMBER or RED notifications being sent to groups of Federation participants and Federation operators?
    c. Has technical.edugain.org been updated to publish Fed ops security contact info? Is there a process to maintain that info?
    d. The IR Handbook says that an AMBER after-action report should be sent to all Sirtfi compliant orgs in all federations affected by the incident. Should a GREEN or WHITE after-action report be published, eg, on the sirtfi.org website?
    e. Slack/Mattermost channel used by the IR team, as a place for IR participants to ask questions and coordinate?
    f. Fed ops incorporate into their security procedures/policies?
    g. Other?
3. Does the WG believe that the above sufficiently fulfills its deliverable of “Define incident response procedures for federations, including communication templates, and support the community in their adoption”?
4. AOB

The WG completed its review of the eduGAIN Security Incident Response Handbook, reflected in comments and changes to the text. Item 2.d above was also addressed in Doc 2 by adding that step to the eduGAIN Security Team’s procedure.