SIRTFI

- Group Tools:
- Group Documents:
- Presentations:
- Face to Face Meetings:
- Virtual Meetings:
- Calendar:
- Training Material/Outreach Inventory:
- External Resources:

The SIRTFI group is looking at processes for expressing security incident handling requirements as an assurance profile for federations and other requirements needed to effectively deploy and enhance incident response processes for FIM. This wiki page details information relating to that work.

The work of this group has been divided into three main phases:

Phase	Description	Work Items	Status
Phase 1	Develop the SIRTFI Trust Framework specification, which defines basic security incident response capabilities to which member organizations can self-assert compliance. This initial draft is intended to be a simplified framework that lays the groundwork for how such an approach should be defined. Significant effort will be needed to understand how this might be deployed in the existing R&E FIM environment.	~~Draft SIRTFI document for consultation.~~ ~~Consultation to support development of public v1.0.~~ ~~Decide whether IdP notification of compromised account belongs in v1.0 or will be slated for v2.0 in alignment with Phase 3 work.~~ ~~Propose / finalise entity metadata schema for security contacts.~~ ~~Propose / finalise entity attribute profile to signify adherence with Sirtfi public v1.0.~~	COMPLETE SIRTFI Consultation: Framework Sirtfi v1.0 approved by the REFEDS steering committee and published. Metadata extensions confirmed Guide for Federation Participants Sirtfi added to IANA assurance profiles registry. https://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml
Phase 2	Establish the means by which member organisations in all R&E federations can indicate their compliance with the SIRTFI Trust Framework, how they can be contacted to participate in a coordinated response to a federated security incident. Define the roles and responsibilities of the various parties in managing federated security incidents, information sharing guidelines, tools, procedures, and templates.	~~Produce educational and communication materials for REFEDS to promulgate to member R&E federations.~~ ~~Promulgate educational and communication materials to help R&E federations to promote and support Sirtfi public v1.0 adoption.~~ ~~Test incident response process and use of security contact metadata in simulated activity.~~ ~~Implement processes by which to maintain and broadcast security contact information and Sirtfi trust framework adherence, outside standard federation metadata publication mechanisms.~~ ~~Establish communication channels for security information exchange and incident report sharing.~~ ~~Define incident response procedures for federations, including communication templates, and support the community in their adoption.~~ ~~Implement metadata extension for security contact information.~~ ~~Implement metadata profile to signify Sirtfi public v1.0 adherence.~~	COMPLETE Homepage https://refeds.org/sirtfi Metadata Guide for Federation Participants Moodle training course for Sirtfi developed under AARC Two annual table top exercises GN4-2 will support tools for maintaining security contacts and monitoring adherence. Survey and analysis of tool usage are in IR Communication Tools folder within the Sirtfi WG folder. The WG concluded that it is unrealistic to expect IR teams already using such tools within their domains to switch or use additional tools. The Sirtfi+ Registry concept was developed and pilot implementation occurred through the Geant incubator task. Interest in this work by its sponsors waned. The eduGAIN Security Incident Response Handbook was developed in partnership with the eduGAIN Security Team. Several incident response templates were developed. These have been suggested as starting points for use by the eduGAIN Security Team. Table top testing has been taken up by the Security Communications Challenge Coordination Joint Working Group.

Phase 3	Establish the means for proactive notification of an account compromise when it can be expected to produce a substantial impact to an at-risk SP organisation.	~~Analyse suitability of existing identity event notification solutions such as IETF's Security Events to R&E federations, and potentially define and set up means for IdP organizations to issue events related to account compromises to SPs registered as at-risk.~~ ~~Develop tools to help IdPs identify accounts that have been used to access specified SPs.~~ ~~Define Sirtfi version 2 to include the requirement to notify affected participating organisations of security incidents~~ ~~Promote testing responsiveness of security contact information by federation operators or other parties.~~	COMPLETE Sirtfi version 2. Struck "Develop tools to help IdPs identify accounts that have been used to access specified SPs." as being unrealistic and of low value. It was decided that responsiveness testing is better addressed by eduGAIN and individual R&E federations. Cf. Recommendation 1.1 of the eduGAIN Futures report. It was decided that the huge effort required to implement an automated IETF security events infrastructure across R&E federation members globally would be better applied towards larger objectives, like Baseline Expectations. Further, as federated entities rely increasingly on commercial systems, those systems would need to be modified to integrate with such an infrastructure, a prospect considered to be unlikely.

Group Tools:

Mailing list archive: https://www.terena.org/mail-archives/sirtfi/threads.html. has been migrated to https://lists.refeds.org/sympa/info/sirtfi. Join the SIRTFI list at: https://lists.refeds.org/sympa/info/sirtfi.

Technical Training Wiki: SIRTFI Home

Security Contact Metadata Extension: Security Contact Metadata Extension Schema

Sirtfi Home Page (Public Facing): https://refeds.org/sirtfi

Google WG folder: https://drive.google.com/drive/folders/1_4zo_qJdqz1ugZD9MfPUKt_OID6elHVr?usp=sharing

Group Documents:

- https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf The published version of Sirtfi 1.0
- http://goo.gl/2xnf2G is the old working document for the framework on Google Docs.
- Proposed workplan.
- Sirtfi Normative Description: https://refeds.org/wp-content/uploads/2016/11/Sirtfi-certification-v1.0.pdf
- GN4 Sirtfi Interview Survey Report
- SIRTFI+ Registry Requirements
- IR Handbook Consultation response.xlsx
- eduGAIN Security Incident Response Handbook v1.0
- Act-Inform diagram
- Sirtfi v2 The published version of Sirtfi 2.0
- Sirtfi v2 Benefits
- Coexistence of Sirtfi v1 and Sirtfi v2

Presentations:

SIRTFI has been presented at the following events:

- FIM4R BoF at TNC2014.
- REFEDS, October 2014.
- FIM4R, CERN, February 2015.
- TechEx, Cleveland, October 2015
- FIM4R, EWTI, December 2015
- Kantara, Working Group Special meeting, April 2016
- Internet2 Webinar, May 2016
- TF-CSIRT, May 2016
- AARC Meeting, Incident Response, May 2016
- SWITCH ICT Focus, November 2016
- IAMOnline Europe, March 2017
- WISE, March 2017
- TNC17, May 2017
- DeIC Conference, September 2017
- TNC18, June 2018
- REFEDS @ TechEX, October 2018
- HOW19, March 2019

Face to Face Meetings:

- 8th June 2014 in Amsterdam, Netherlands.
- Morning of 31st October 2014 in Indianapolis, Indiana.
- 17 June 2015, informal gathering during TNC 2015

- 6 October 2015, informal gathering during TechEx
- 28 September 2016, ACAMP Session
- 22nd February 2017, TIIME Workshop Session

Virtual Meetings:

- 1st October 2014 at 16.30 CEST via Skype.
- 29th January 2015 via Skype.
- 14th December 2015 via Vidyo, Consultation Feedback and Changes
- 25th January 2016 via Vidyo
- 18th April 2016 via Vidyo SIRTFI
- 6th July 2016 via Vidyo SIRTFI
- 9th August 2016 via Vidyo SIRTFI
- 2nd November 2016 via Vidyo Sirtfi Normative Description Consultation Followup
- 9th Feb 2017 via Vidyo SIRTFI
- 12th of July 2017 via Vidyo SIRTFI
- 7th of August 2017 via Vidyo Sirtfi Call August 2017.pdf
- 2nd of October 2017 via Vidyo Sirtfi Call September 2017
- 4th of December 2017 via Vidyo Notes Sirtfi Call December 4th 16_00.pdf
- 29th of January 2018 via Bluejeans Sirtfi Registry Call 29_01_2018.pdf
- 14th of April 2018 via Bluejeans 20180412 Sirtfi WG call notes.pdf
- 28th April 2018 via Zoom 20180426 Sirtfi WG call notes.pdf
- 10th May 2018 via Zoom 20180510 Sirtfi WG call notes.pdf
- 24th May 2018 via Zoom 20180524 Sirtfi WG call notes.pdf
- 7th June 2018 via Zoom 20180607 Sirtfi WG call notes.pdf
- 21st June 2018 via Zoom 20180621 Sirtfi WG call notes.pdf
- 5th July 2018 via Zoom 20180705 Sirtfi WG call notes.pdf
- 2nd August 2018 via Zoom 20180802 Sirtfi WG call notes.pdf
- 16th August 2018 via Zoom 20180816 Sirtfi WG call notes.pdf
- 30th August 2018 via Zoom 20180830 Sirtfi WG call notes.pdf
- 27th September 2018 via Zoom 20180927 Sirtfi WG call notes.pdf
- 11th October 2018 via Zoom 20181011 Sirtfi WG call notes.pdf
- 25th October 2018 via Zoom 20181025 Sirtfi WG call notes.pdf
- 8th November 2018 via Zoom 20181108 Sirtfi WG call notes.pdf
- 6th December 2018 via Zoom 20181206 Sirtfi WG call notes.pdf
- 20th December 2018 via Zoom 20181220 Sirtfi WG call notes.pdf
- 17th January 2019 via Zoom 20190117 Sirtfi WG call notes.pdf
- 31 January 2019 via Zoom 20190131 Sirtfi call notes.pdf
- 28 February 2019 via Zoom 20190228 Sirtfi call notes .pdf
- 14 March 2019 via Zoom Sirtfi call notes 20190314.pdf
- 28 March 2019 via Zoom Sirtfi call notes 20190328.pdf
- 11 April 2019 via Zoom 20190411 Sirtfi call notes.pdf
- 25 April 2019 via Zoom 20190425 Sirtfi call notes.pdf
- 9 May 2019 via Zoom 20190509 Sirtfi call notes.pdf
- 23 May 2019 via Zoom 20190523 Sirtfi call notes
- 6 June 2019 via Zoom 20190606 Sirtfi call notes
- 4 July 2019 via Zoom 20190704 Sirtfi call notes
- 18 July 2019 via Zoom 20190718 Sirtfi call notes
- 1 August 2019 via Zoom 20190801 Sirtfi call notes
- 20190815 Sirtfi call notes
- 20190829 Sirtfi call notes
- 20191010 Sirtfi call notes
- 20191024 Sirtfi call notes
- 20191107 cancelled
- 20191121 Sirtfi call notes
- 20191205 Sirtfi call notes
- 20191219 Sirtfi call notes
- 20200115 Sirtfi call notes
- 20200130 Sirtfi call notes
- 20200213 Sirtfi call notes
- 20200227 Sirtfi call notes
- 20200312 Sirtfi call notes
- 20200326 Sirtfi call notes
- 20200409 Sirtfi call notes
- 20200423 Sirtfi call notes
- 20200507 Sirtfi call notes
- 20200521 Sirtfi call notes
- 20200604 Sirtfi call notes
- 20200616 Sirtfi call notes
- 20200716 Sirtfi call notes
- 20200730 Sirtfi call notes
- 20200813 Sirtfi call notes
- 20200827 Sirtfi call notes
- 20200910 Sirtfi call notes
- 20200924 Sirtfi call notes
- 20201008 Sirtfi call notes
- 20201022 Sirtfi call notes
- 20201105 Sirtfi call notes

- 20201203 Sirtfi call notes
- 20201217 Sirtfi call notes
- 20210114 Sirtfi call notes
- 20210128 Sirtfi call notes
- 20210211 Sirtfi call notes
- 20210225 Sirtfi call notes
- 20210311 Sirtfi call notes
- 20210325 Sirtfi call notes
- 20210408 Sirtfi call notes
- 20210422 Sirtfi call notes
- 20210603 Sirtfi call notes
- 20210617 Sirtfi call notes
- 20210701 Sirtfi call notes
- 20210715 Sirtfi call notes
- 20210729 Sirtfi call notes
- 20210812 Sirtfi call notes
- 20210909 Sirtfi call notes
- 20210923 Sirtfi call notes
- 20211104 Sirtfi call notes
- 20211118 Sirtfi call notes
- 20211202 Sirtfi call notes
- 20211216 Sirtfi call notes
- 20220113 Sirtfi call notes
- 20220127 Sirtfi call notes
- 20220210 Sirtfi call notes
- 20220224 Sirtfi call notes
- 20220310 Sirtfi call notes
- 22020324 Sirtfi call notes
- 20220421 Sirtfi call notes
- 20220505 Sirtfi call notes
- 20220519 Sirtfi call notes
- 20220602 Sirtfi call notes
- 20220630 Sirtfi call notes
- 20220714 Sirtfi call notes
- 20220728 Sirtfi call notes
- 20220811 Sirtfi call notes
- 20220922 Sirtfi call notes
- 20221006 Sirtfi call notes

Calendar:

Team Calendars

Training Material/Outreach Inventory:

Material	Audience	Format	Link
Benefits of Sirtfi	All	PDF	https://refeds.org/wp-content/uploads/2016/02/Why_Sirtfi.pdf
Technical changes	Fed Ops	Wiki	Guide for Federation Operators
Outreach Package	Fed Ops	Wiki	Guide for Federation Operators#SampleOutreachLetterforFederationParticipants
Steps to follow	Entities	Web Page	Guide for Federation Participants
FAQs	Entities	Web Page	General: https://refeds.org/sirtfi/sirtfi-faqs Technical: FAQs

Logo (to act as a trust mark on compliant sites)	Entities	Image	 SIRTFI_logo.eps
Sirtfi Framework Doc	All	PDF on Web Page	https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf
Summary poster	All	Poster	SIRTFI
Sirtfi emailer helper	End users	Web page	http://sirtfi.cern.ch
Sirtfi Moodle Course	Entities	Moodle	https://e-academy.geant.org/moodle/course/view.php?id=2

External Resources:

- http://www.cic.net/docs/default-source/technology/federated_security_incident_response.pdf
- https://spaces.internet2.edu/display/InCFederation/Federated+Security+Incident+Response
- https://edms.cern.ch/file/428035/7/SecurityIncidentResponse-v3.2a.pdf
- https://stix.mitre.org/
- http://cybox.mitre.org
- http://maec.mitre.org/
- http://taxii.mitre.org/
- https://github.com/berggren/fordrop
- http://www.timesketch.org/
- https://community.ja.net/blogs/regulatory-developments/article/cleaning-after-botnets
- http://googleonlinesecurity.blogspot.com/2014/09/cleaning-up-after-password-dumps.html
- https://docs.google.com/a/google.com/presentation/d/1ivU3fVCjBBZrguCfgY237BAjZ3Rp_MRGtoh2dxVypds/edit?pli=1#slide=id.g24243b4f_044
- https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting.https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting.