All is calm at your local security team.

Too calm.

Hmmm. This user is acting very strangely

Which user?

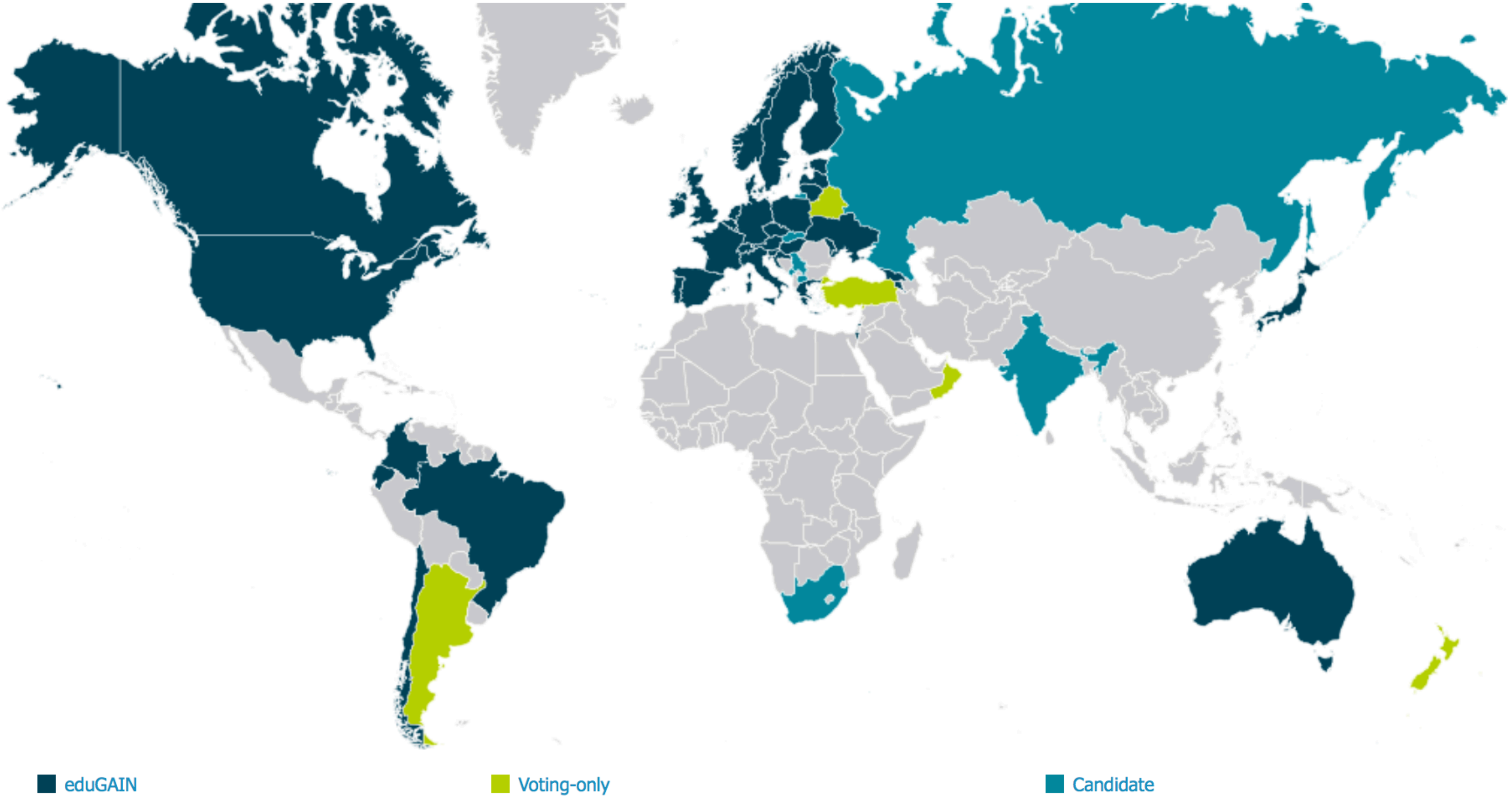
It's one of our external users, coming in through eduGAIN

Think they're compromised? Can we reach security at their home organisation?

No! All we have is a billing contact...

What if…?

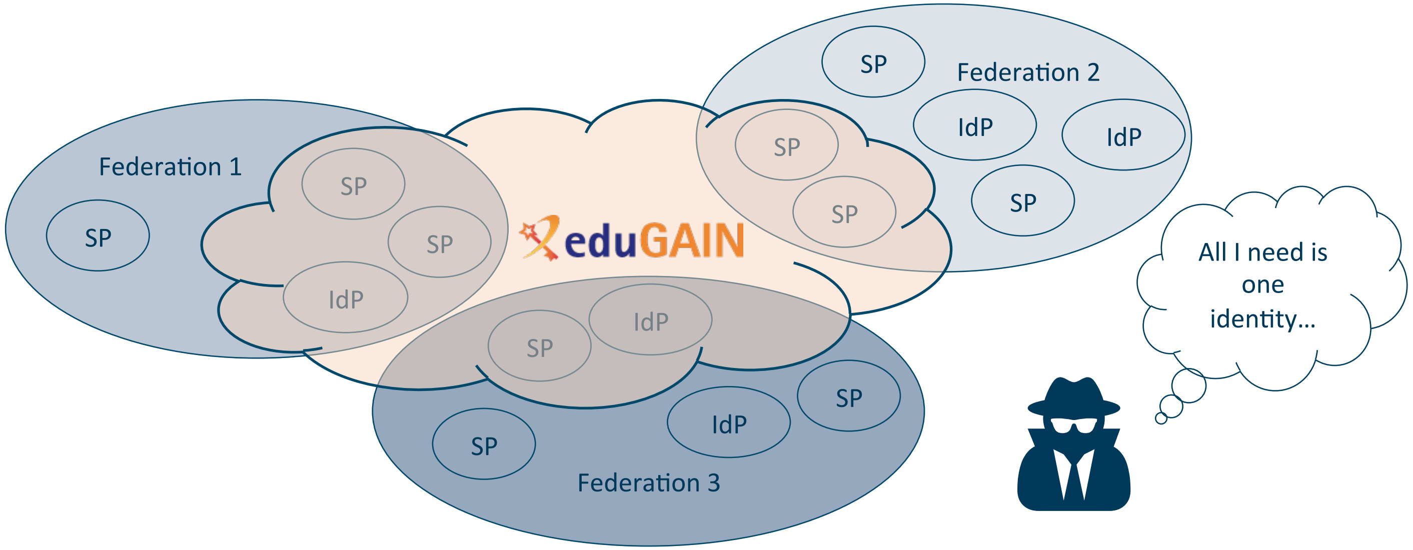
… an incident spread throughout the federated R&E community via a single compromised identity?



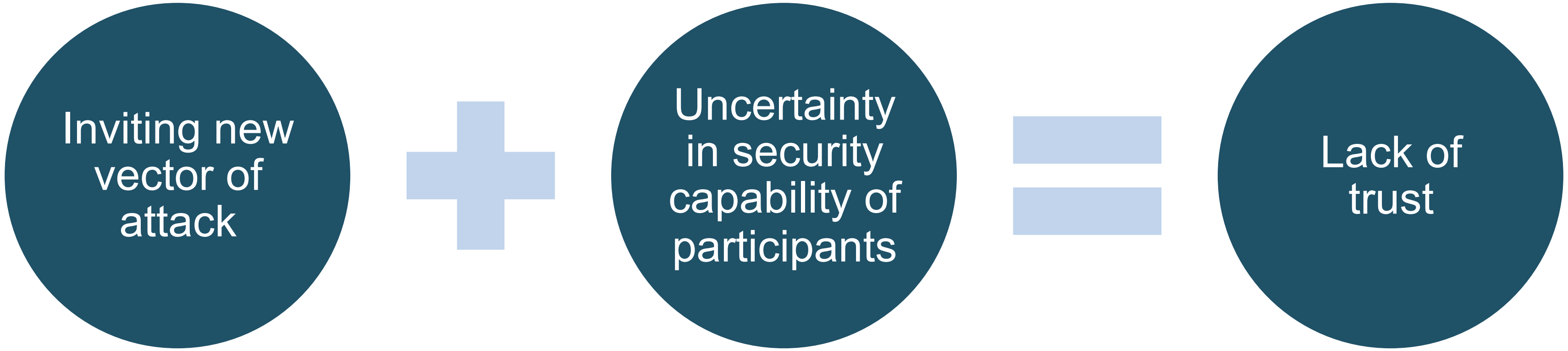
https://technical.edugain.org/

Federated Security Incident Response
The problem

- Clearly an inviting vector of attack
- The lack of a centralised support system for security incident response is an identified risk to the success of eduGAIN
- We will need organisations to collaborate during incident response – this may be outside their remit



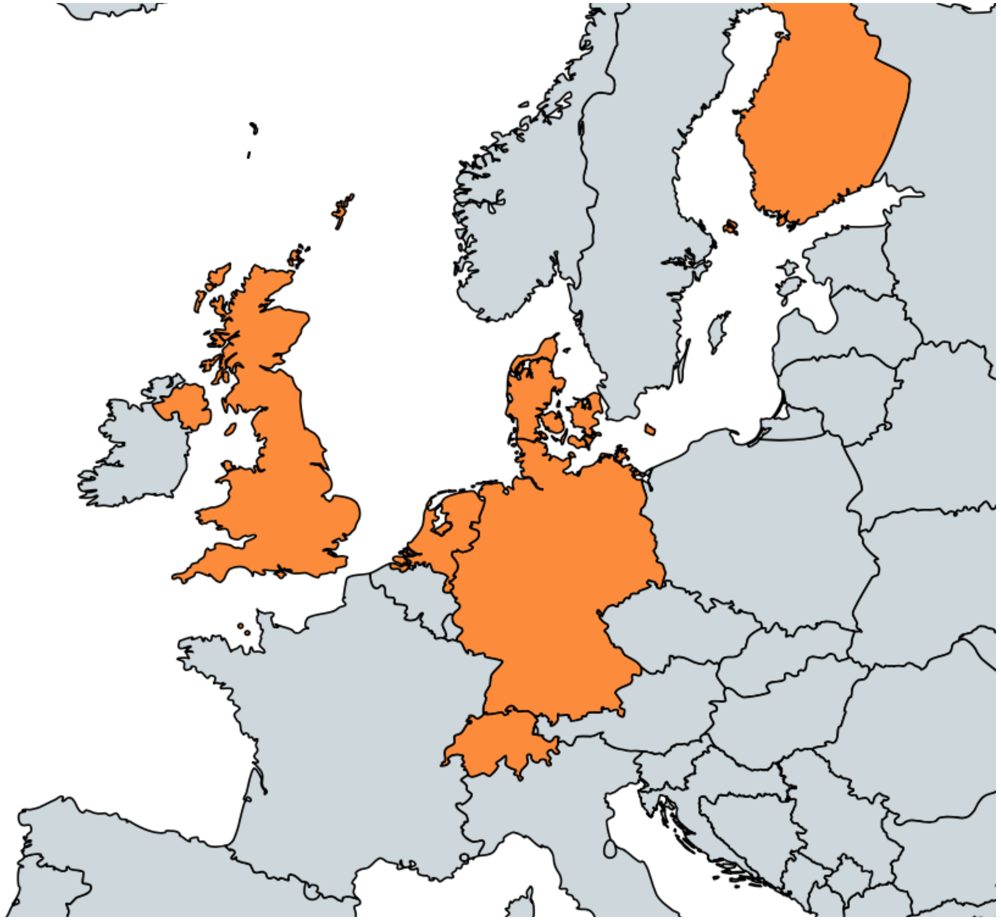
Federated Security Incident Response
The solution


Inviting new vector of attack
+
Uncertainty in security capability of participants
=
Lack of trust

- Attacks are inevitable ☹
- But we can make security capability transparent and build relationships between organisations and people ☺

We need a **S**ecurity **I**ncident **R**esponse **T**rust Framework for **F**ederated **I**dentity, **Sirtfi**!

Who is in?



Who's doing the work?

- REFEDS Working Group
- Groundwork done by the AARC Project
- Handover to GN4 for deployment

Who will be the first to benefit?

- Pilot federations
- Key e-Infrastructures
- Several new services adding Sirtfi as a requirement

Want to find out more?
https://refeds.org/sirtfi

AARC

Sirtfi

A Security Incident Response Trust Framework for Federated Identity

The Security Incident Response Trust Framework for Federated Identity (Sirtfi) provides a mechanism to identify trusted, operationally secure eduGAIN participants and facilitate effective incident response collaboration. Sirtfi has been developed with input from Identity Federation communities worldwide and aims to provide a scalable safeguard against inevitable future attacks.

Is your organization part of an identity federation?
Make security a priority by adopting Sirtfi.

The problem

The growth and inter-connection of federations has created a new vector of attack. One compromised account can provide access to a multitude of services across the inter-federation community.

The quality of operational security at organizations is variable and often unknown to other participants. There is typically no minimum level of security to join a federation. Consequently, there is no guarantee of effective collaboration between organizations in the event of an inevitable federated incident.

The Problem: organizations are choosing to opt out of eduGAIN, or block authentication, due to lack of trust.

The solution

Since a centrally coordinated incident response capability within the community does not exist, participants must collaborate to mitigate the risk of incidents.

Sirtfi describes practices and attributes that identify an organization as being capable of participating effectively in incident response. The framework stipulates preventative measures to protect an organization from attack, and behaviour to adopt in the event of an incident. By adopting Sirtfi, an organization asserts that it can meet the following points:

Operational Security
- Provide security incident response capability with sufficient authority to mitigate, contain the spread of, and remediate the effects of an incident.

Incident Response
- Assure confidentiality of information exchanged
- Identify trusted security contacts
- Guarantee a response during collaboration

Traceability
- Record and share relevant system generated information
- Ensure such information is kept
policy

Participant Responsibilities
- Confirm that end users are awa
AUP

The Solution: a Trust Framewo

Why should I join?

Sirtfi is used as an identifier to mark trusted partners within eduGAIN. Compliance is expressed in metadata and gives a transparent view of those organizations willing to engage in collaborative incident response.

The credibility gained by asserting Sirtfi compliance opens doors within eduGAIN as organizations choose to enable authentication based on this enhanced trust.

IdPs Gain **access** to useful services that only allow authentication from Sirtfi compliant IdPs	SPs Gain **users** whose home organizations only allow authentication at Sirtfi compliant SPs
Guarantee an efficient and effective **response** from partner organizations during incident response	
Raise the bar in operational **security** across eduGAIN	

How can I j

Are you part of an identity federation? Just fol
- ❑ Test your organization
  Ensure that your organization satisfies eve
- ❑ Choose a Sirtfi Contact
  Use the flowchart below to help!
- ❑ Assert your compliance
  Work with your Federation Operator to add

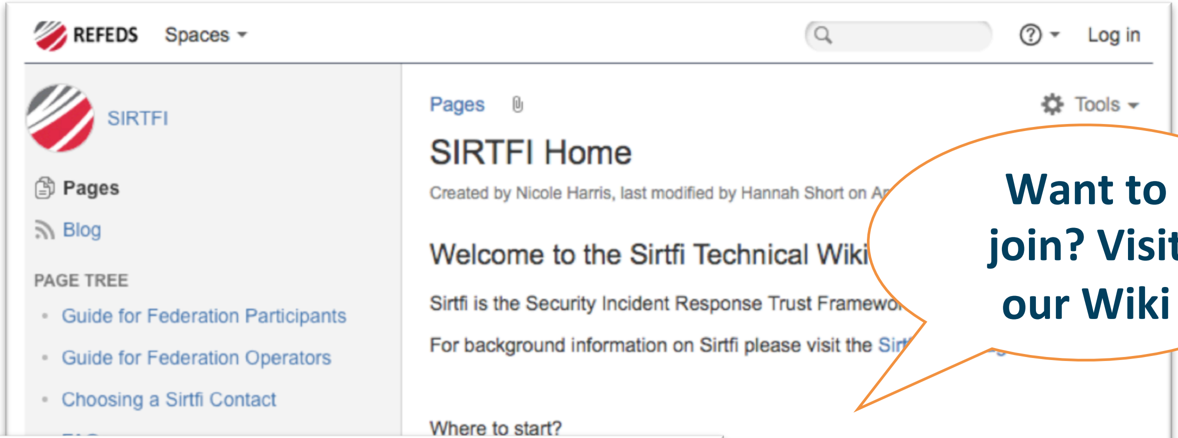
Is my organisation S compliant?
Yes
Is my organisation covered by an external incident response team?
Yes
No
Do they agree to support Sirtfi on behalf of my organisation?
No
Yes
Does my organisation hav security (or equivalen
Yes
Does this team have suff FIM knowledge to support
Yes
External Security Team
Organisation's Securi Team

Get started at h

AARC eduGAIN

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965, **AARC** (Authentication and Authorisation for Research and Collaboration)

We have a poster at TNC!



PAGE TREE

- Guide for Federation Participants
- Guide for Federation Operators
- Choosing a Sirtfi Contact

Pages

SIRTFI Home

Created by Nicole Harris, last modified by Hannah Short on Ap

Welcome to the Sirtfi Technical Wiki

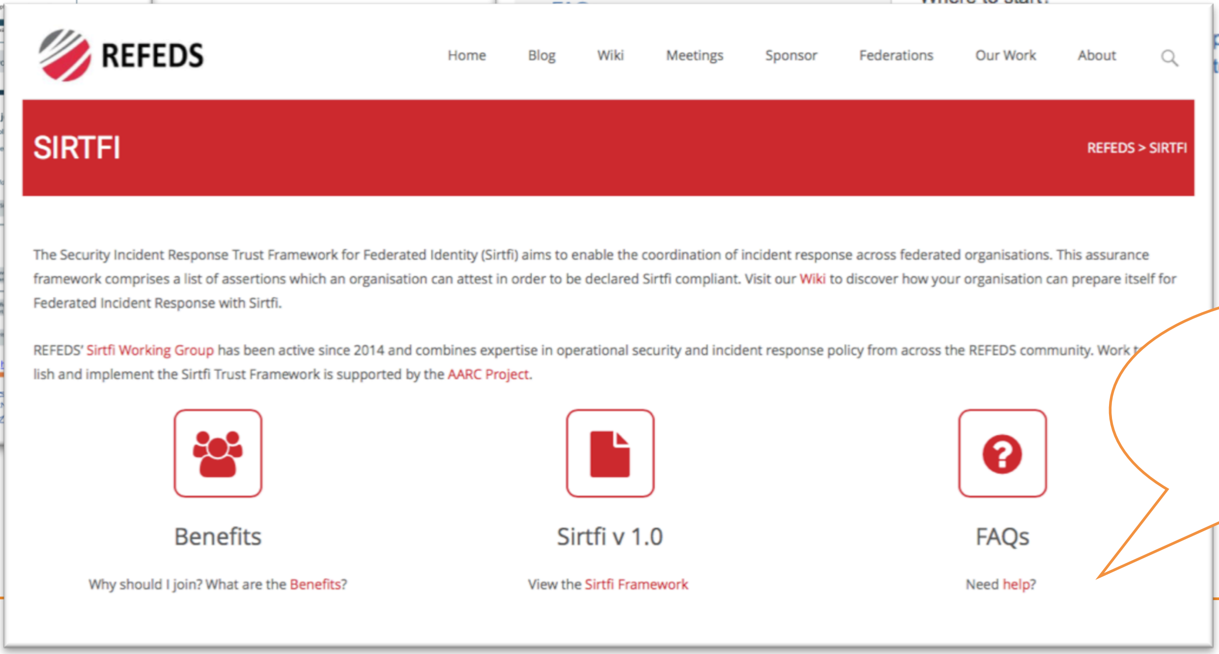
Sirtfi is the Security Incident Response Trust Framewo

For background information on Sirtfi please visit the Sir

Where to start?

pants
tors

Want to join? Visit our Wiki



SIRTFI

REFEDS > SIRTFI

The Security Incident Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response across federated organisations. This assurance framework comprises a list of assertions which an organisation can attest in order to be declared Sirtfi compliant. Visit our Wiki to discover how your organisation can prepare itself for Federated Incident Response with Sirtfi.

REFEDS' Sirtfi Working Group has been active since 2014 and combines expertise in operational security and incident response policy from across the REFEDS community. Work t
lish and implement the Sirtfi Trust Framework is supported by the AARC Project.

Benefits

Why should I join? What are the Benefits?

Sirtfi v 1.0

View the Sirtfi Framework

FAQs

Need help?

Curious? Visit our homepage

Thank you

Any Questions?

hannah.short@cern.ch

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).