Authentication and Authorisation for Research and Collaboration

An introduction to Sirtfi

Addressing Federated Security Incident Response

Hannah Short
CERN
hannah.short@cern.ch

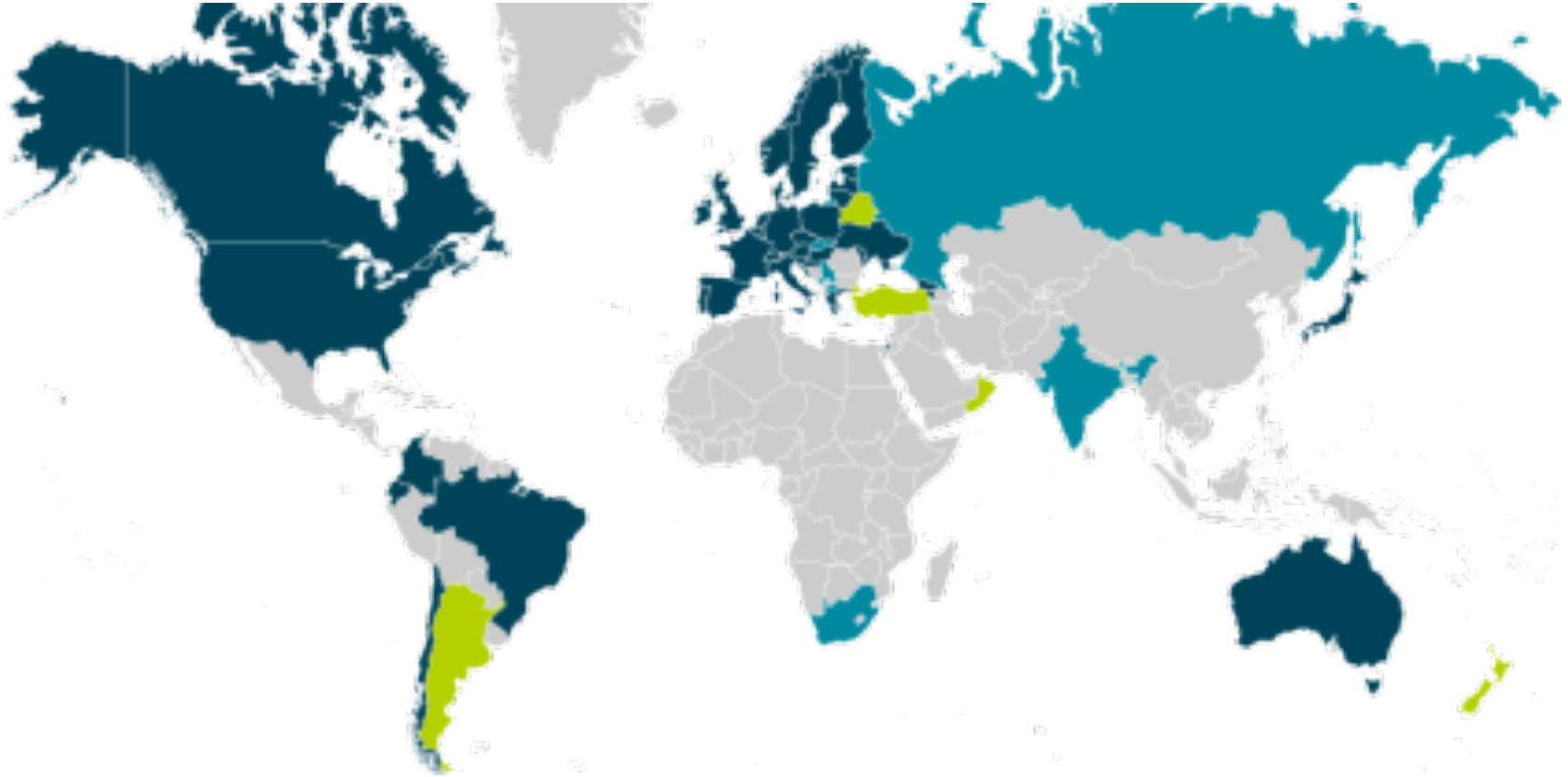
TF-CSIRT
May, 2016

Agenda

- Federated Security Incident Response
  - The problem
  - The solution
- Security Incident Response Trust Framework for Federation Identity Management
  - A history
  - Trust Framework Requirements
- Sirtfi
  - Metadata
  - Find out more

What if…?

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



https://technical.edugain.org/

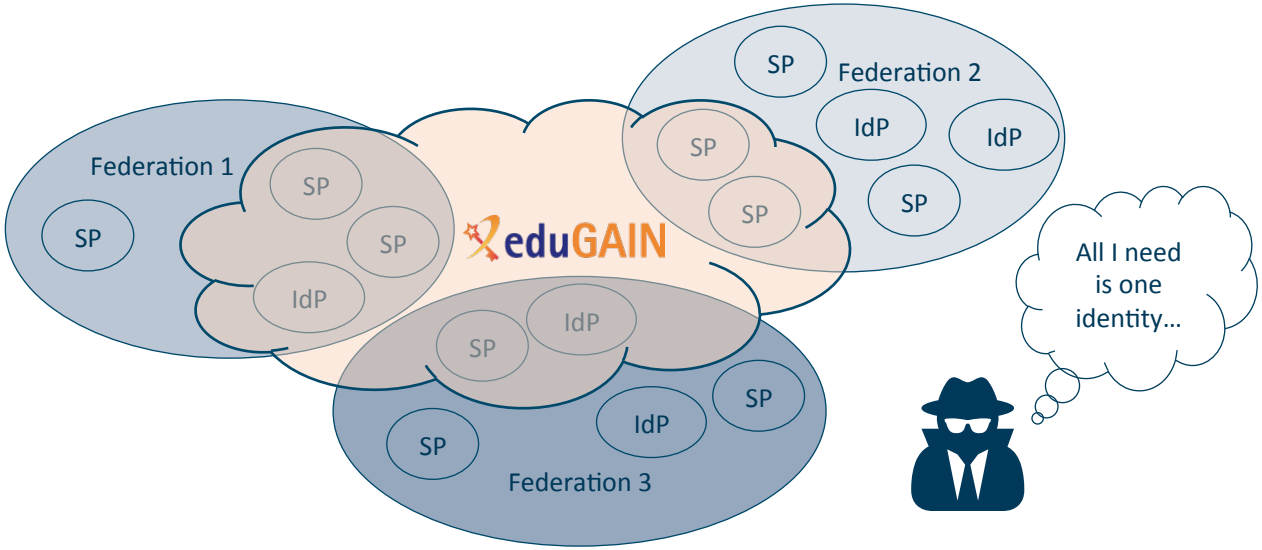
Federated Security Incident Response
What if…?

- How could we determine the scale of the incident?
  - Do useful logs exist?
  - Could logs be shared?
- Who should take responsibility for resolving the incident?
- How could we alert the identity providers and service providers involved?
- Could we ensure that information is shared confidentially, and reputations protected?

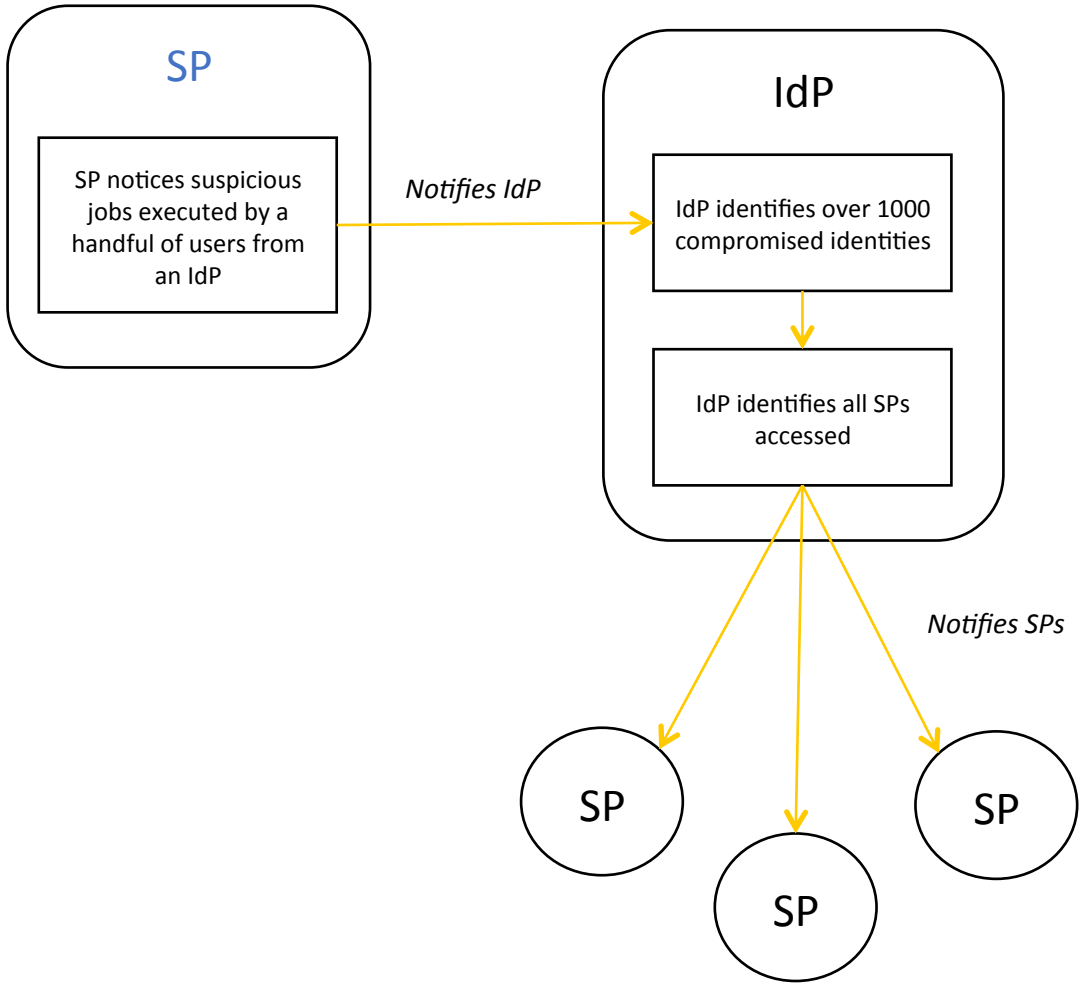
eduGAIN numbers	
Federations:	38
All entities:	3232
IdPs:	2037
SPs:	1197
Standalone AAs:	3

Federated Security Incident Response
The problem

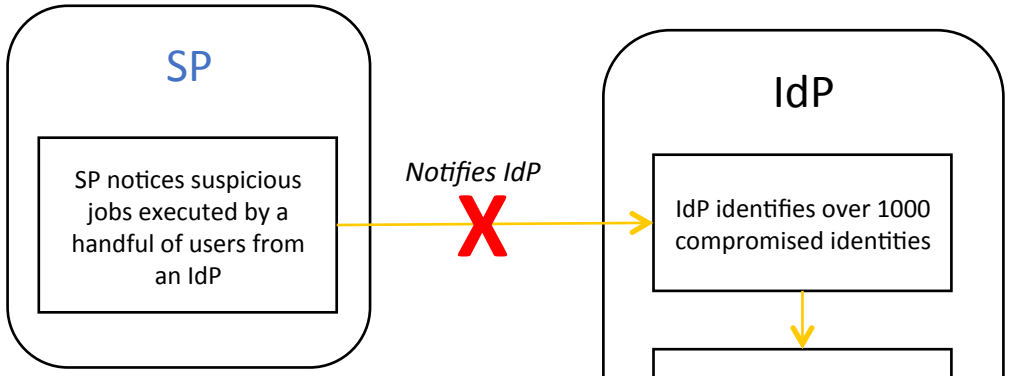
- Clearly an inviting vector of attack
- The lack of a centralised support system for security incident response is an identified risk to the success of eduGAIN
- We will need participants to collaborate during incident response – this may be outside their remit



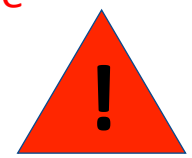
It all seems like common sense…



… but in reality

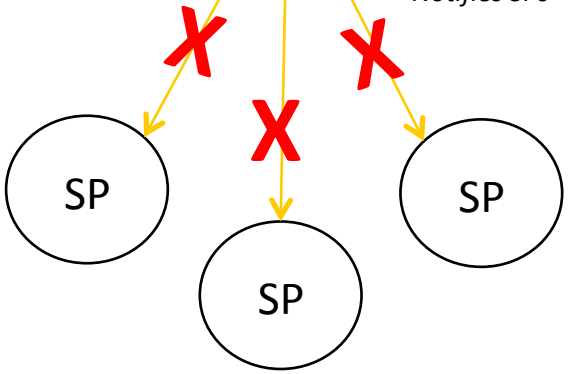


Small IdP may not have capability to block users, or trace their usage



Large SP does not share details of compromise, for fear of damage to reputation

Notifies SPs



SPs are not bound to abide by confidentiality protocol and disclose sensitive information

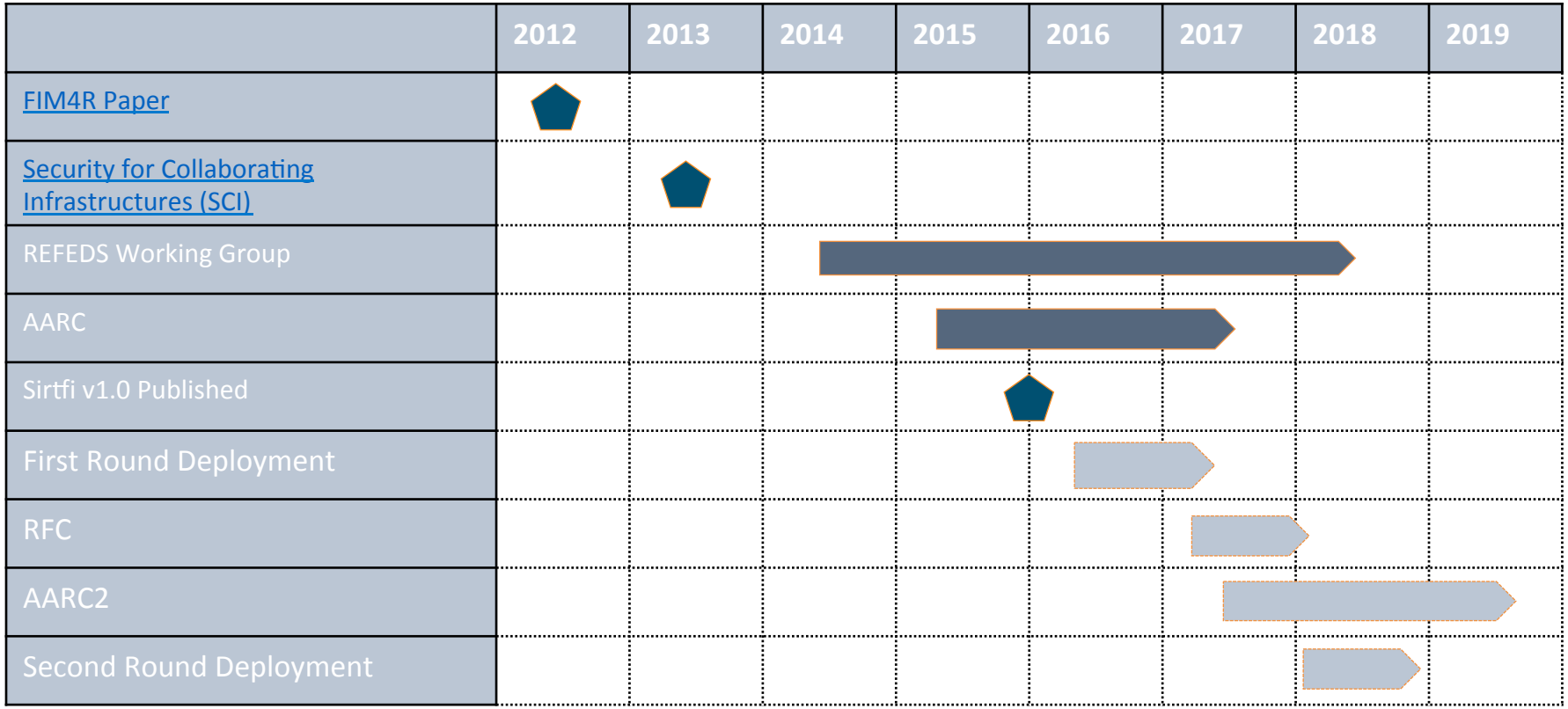
No security contact details!

Federated Security Incident Response
The solution

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

…We need a trust framework!

Security Incident Response Trust Framework for FIM
A history and the future



Security Incident Response Trust Framework for FIM
Sirtfi status

- The SCI document formed the basis for the Security Incident Response Trust Framework for Federated Identity

- ✓ Articulate framework requirements
- ✓ Complete Community Consultation
- ✓ Publish Sirtfi framework
- ✓ Create Training material
- ✓ Confirm metadata extensions
- ❑ Begin adoption
- ❑ Support filtering based on Sirtfi

Security Incident Response Trust Framework for FIM
Sirtfi summary

Operational Security

- Require that a security incident response capability exists 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 contacts
- Guarantee a response during collaboration

Traceability

- Improve the usefulness of logs
- Ensure logs are kept in accordance with policy

Participant Responsibilities

- Confirm that end users are aware of an appropriate AUP

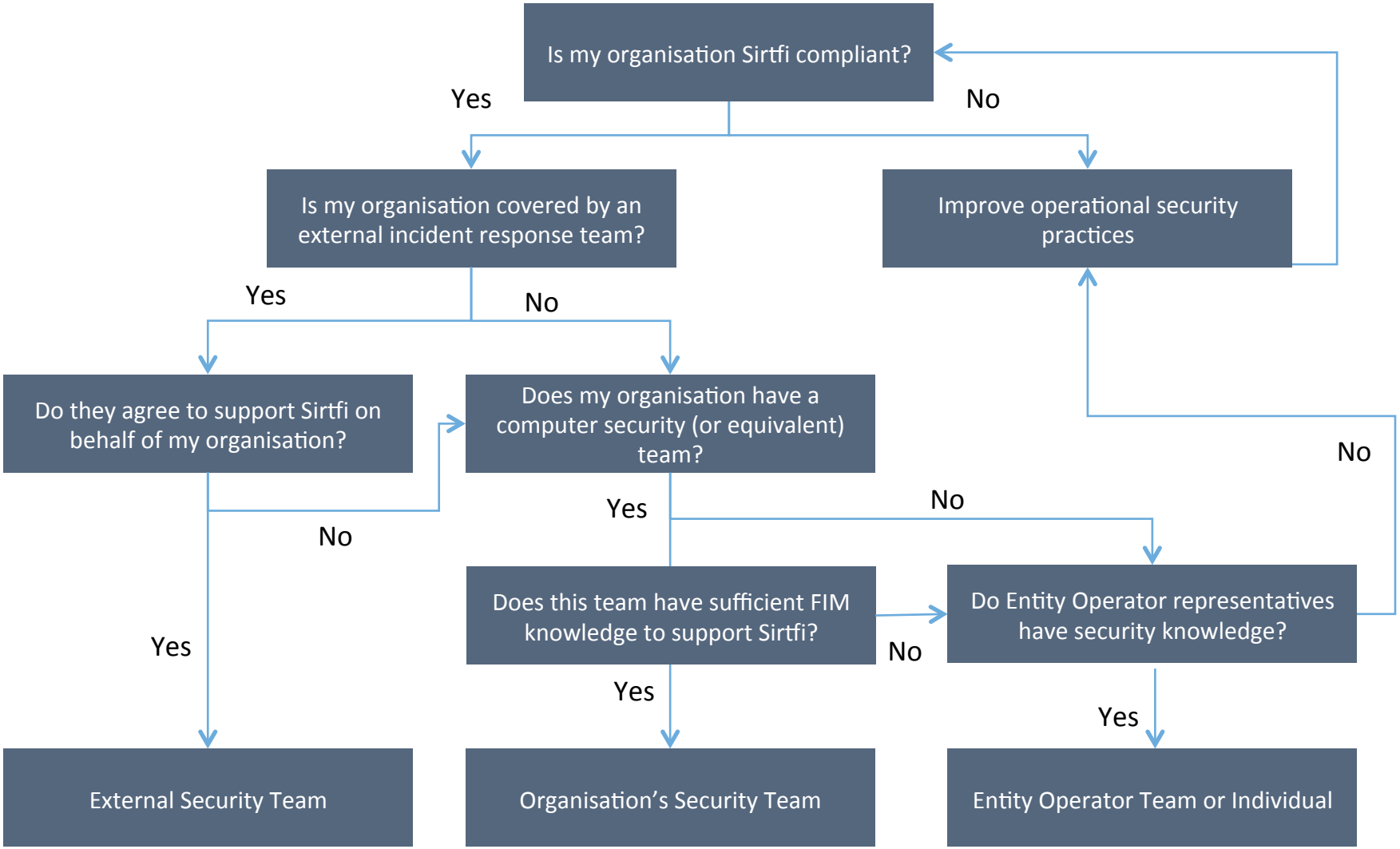
Sirtfi
Security contact details

- Who to choose?
  https://wiki.refeds.org/display/SIRTFI/Choosing+a+Sirtfi+Contact
  - Individual/group who will perform Sirtfi requirements on behalf of the entity (entity = federated identity-provider/service-provider/…)
  - Can leverage CERTs and other existing external teams
- What to include?
  - Mandatory GivenName and EmailAddress
  - Can add additional telephone numbers and email addresses if desired

```
<ContactPerson contactType="other"
          xmlns:remd="http://refeds.org/metadata"
          remd:contactType="http://refeds.org/metadata/contactType/security">
                    <GivenName>Security Response Team</GivenName>
                    <EmailAddress>security@institution.edu</EmailAddress>
</ContactPerson>
```


Credit to David Groep (Nikhef) for this slide

Sirtfi
Security contact choice



Sirtfi
Security contact expectations

Framework requirements

- Use and respect the Traffic Light Protocol (TLP) during all incident response correspondence
- Promptly acknowledge receipt of a security incident report
- As soon as circumstances allow, investigate incident reports regarding resources, services, or identities for which they are responsible

The Sirtfi contact should be the primary point of contact during incident response and is expected to involve secondary contacts as necessary

Sirtfi
Expressing compliance

- Asserting compliance via standard OASIS assurance profile specification
- Applied to register with IANA

```
<attr:EntityAttributes>
   <saml:Attribute
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
         Name="urn:oasis:names:tc:SAML:attribute:assurance-certification”>
            <saml:AttributeValue>https://refeds.org/sirtfi</saml:AttributeValue>
   </saml:Attribute>
</attr:EntityAttributes>
```

Sirtfi
The benefits

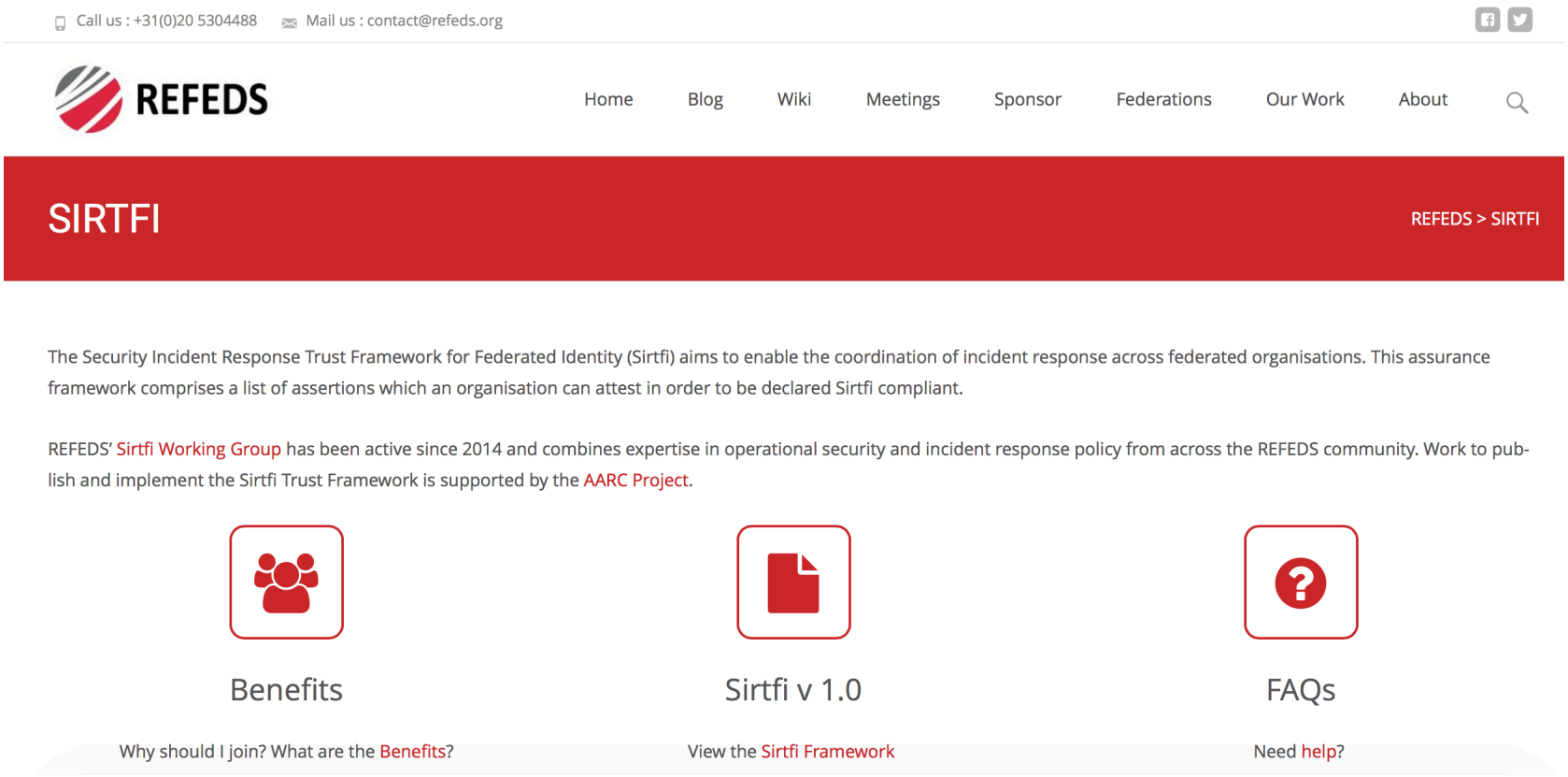
IdPs
Gain **access** to useful services that only allow authentication from Sirtfi compliant IdPs

SPs
Gain **users** whose home organisations only allow authentication at Sirtfi compliant SPs

Guarantee an efficient and effective **response** from partner organisations during incident response

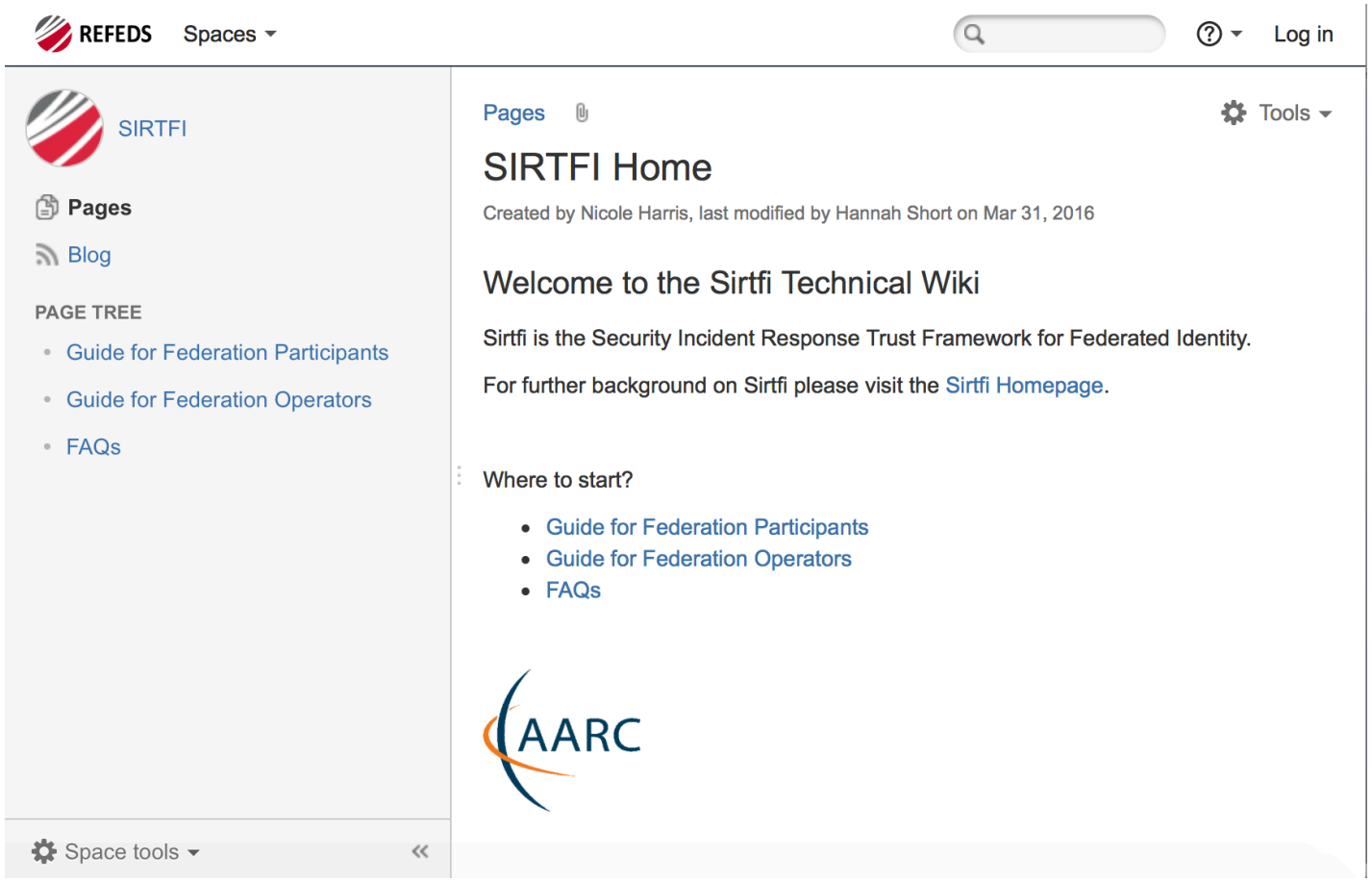
Raise the bar in operational **security** across eduGAIN

Sirtfi
Find out more – Home Page



https://refeds.org/sirtfi

Sirtfi
Find out more – Technical Wiki



https://wiki.refeds.org/display/SIRTFI/SIRTFI+Home

Conclusions

- The Security Incident Response Trust Framework for Federated Identity (Sirtfi) has been developed to address the gap in security response capability within federated computing.
- By creating a sub-network of security conscious entities, and providing contact information for each member, the group raises its mutual trust and is able to establish contact with each other should the need arise.

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).

Appendix, Sirtfi Assertions

Operational security

- [OS1] Security patches in operating system and application software are applied in a timely manner.
- [OS2] A process is used to manage vulnerabilities in software operated by the organisation.
- [OS3] Mechanisms are deployed to detect possible intrusions and protect information systems from significant and immediate threats
- [OS4] A user's access rights can be suspended, modified or terminated in a timely manner.
- [OS5] Users and Service Owners (as defined by ITIL [ITIL]) within the organisation can be contacted.
- [OS6] A security incident response capability exists within the organisation with sufficient authority to mitigate, contain the spread of, and remediate the effects of a security incident.

Incident response

- [IR1] Provide security incident response contact information as may be requested by an R&E federation to which your organization belongs.
- [IR2] Respond to requests for assistance with a security incident from other organisations participating in the Sirtfi trust framework in a timely manner.
- [IR3] Be able and willing to collaborate in the management of a security incident with affected organisations that participate in the Sirtfi trust framework.
- [IR4] Follow security incident response procedures established for the organisation.
- [IR5] Respect user privacy as determined by the organisations policies or legal counsel.
- [IR6] Respect and use the Traffic Light Protocol [TLP] information disclosure policy.

Traceability

- [TR1] Relevant system generated information, including accurate timestamps and identifiers of system components and actors, are retained and available for use in security incident response procedures.
- [TR2] Information attested to in [TR1] is retained in conformance with the organisation's security incident response policy or practices.

Participant responsibilities

- [PR1] The participant has an Acceptable Use Policy (AUP).
- [PR2] There is a process to ensure that all users are aware of and accept the requirement to abide by the AUP, for example during a registration or renewal process.