AARC Authentication and Authorisation for Research and Collaboration

An introduction to Sirtfi

SWITCH ICT Focus

Hannah Short

AARC - Authentication and Authorisation for Research and Collaboration

CERN Computer Security

21st November 2016

SWITCH

With thanks for input from Ann Harding and Thomas Baerecke

Agenda

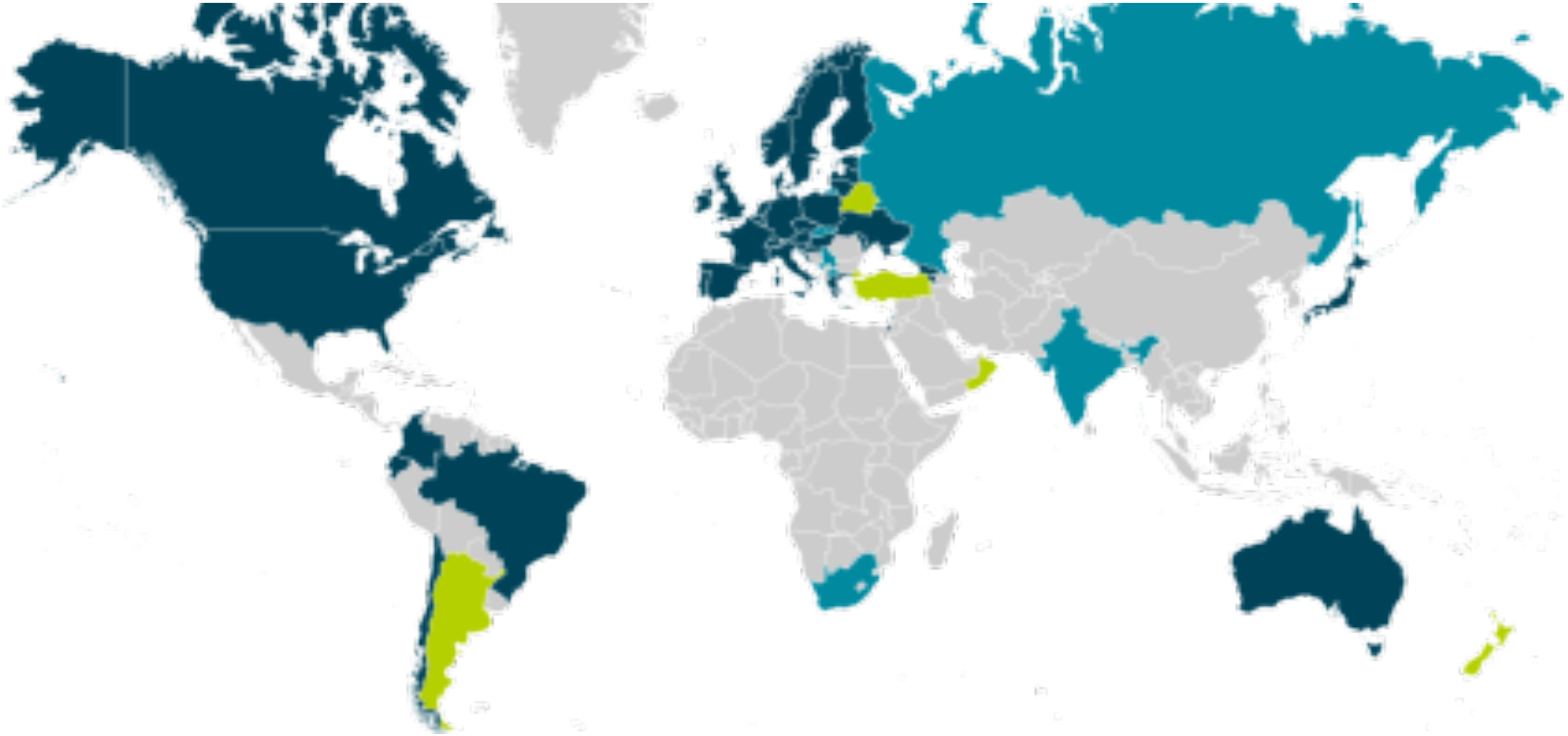
- Federated Security Incident Response
- What is Sirtfi?
- Why is Sirtfi important?
- What do I need to do?
- Where can I look next?

Agenda

- Federated Security Incident Response
- What is Sirtfi?
- Why is Sirtfi important?
- What do I need to do?
- Where can I look next?

What if…?

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



https://technical.edugain.org/

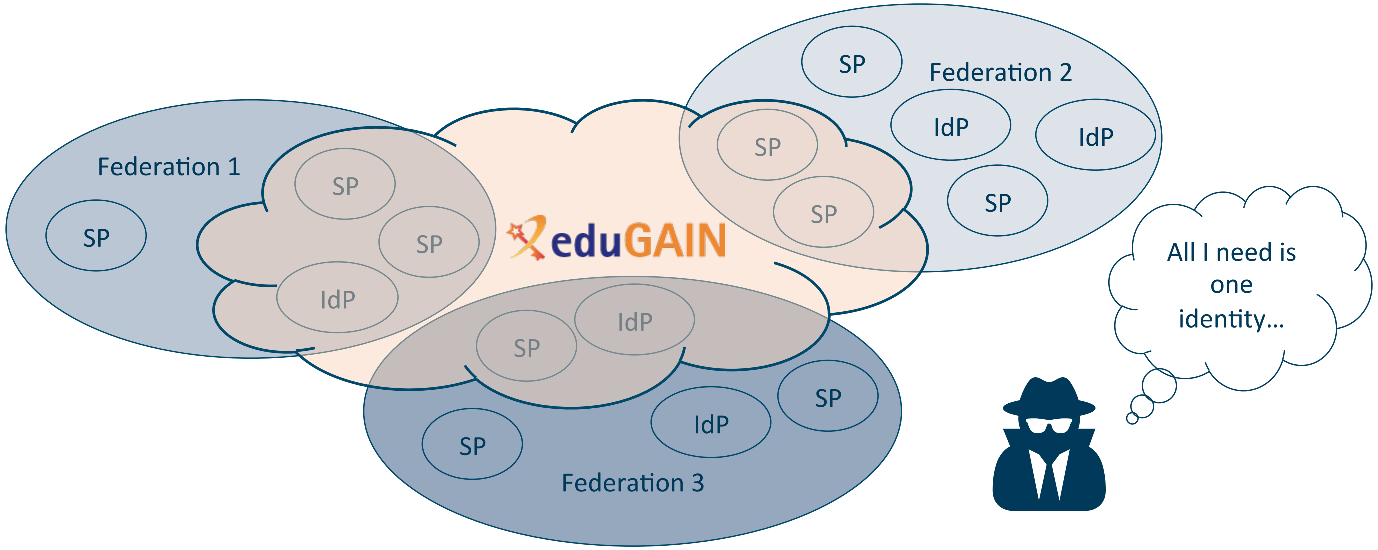
Federated Security Incident Response
What if…?

- 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	**(Oct 2016)**
Federations:	38
All entities:	3591
IdPs:	2220
SPs:	1375
Standalone AAs:	3

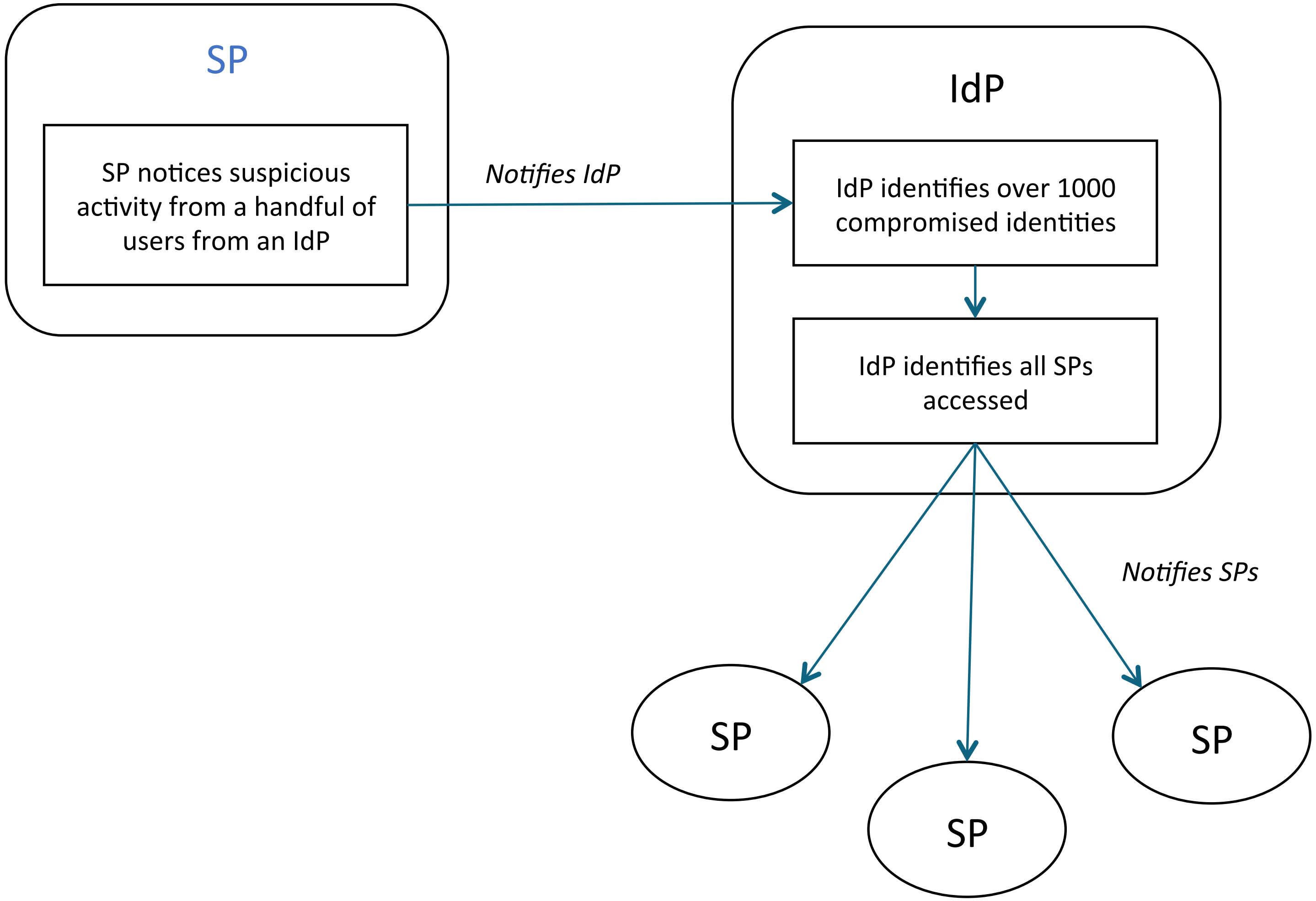
Federated Security Incident Response
The problem

- Although decentralised systems generally mitigate impact of incidents, there is still clearly an inviting vector of attack
- As eduGAIN is invisible to campuses, services and users, there is no central collaboration infrastructure
- We will need participants to collaborate during incident response – this may be outside their remit



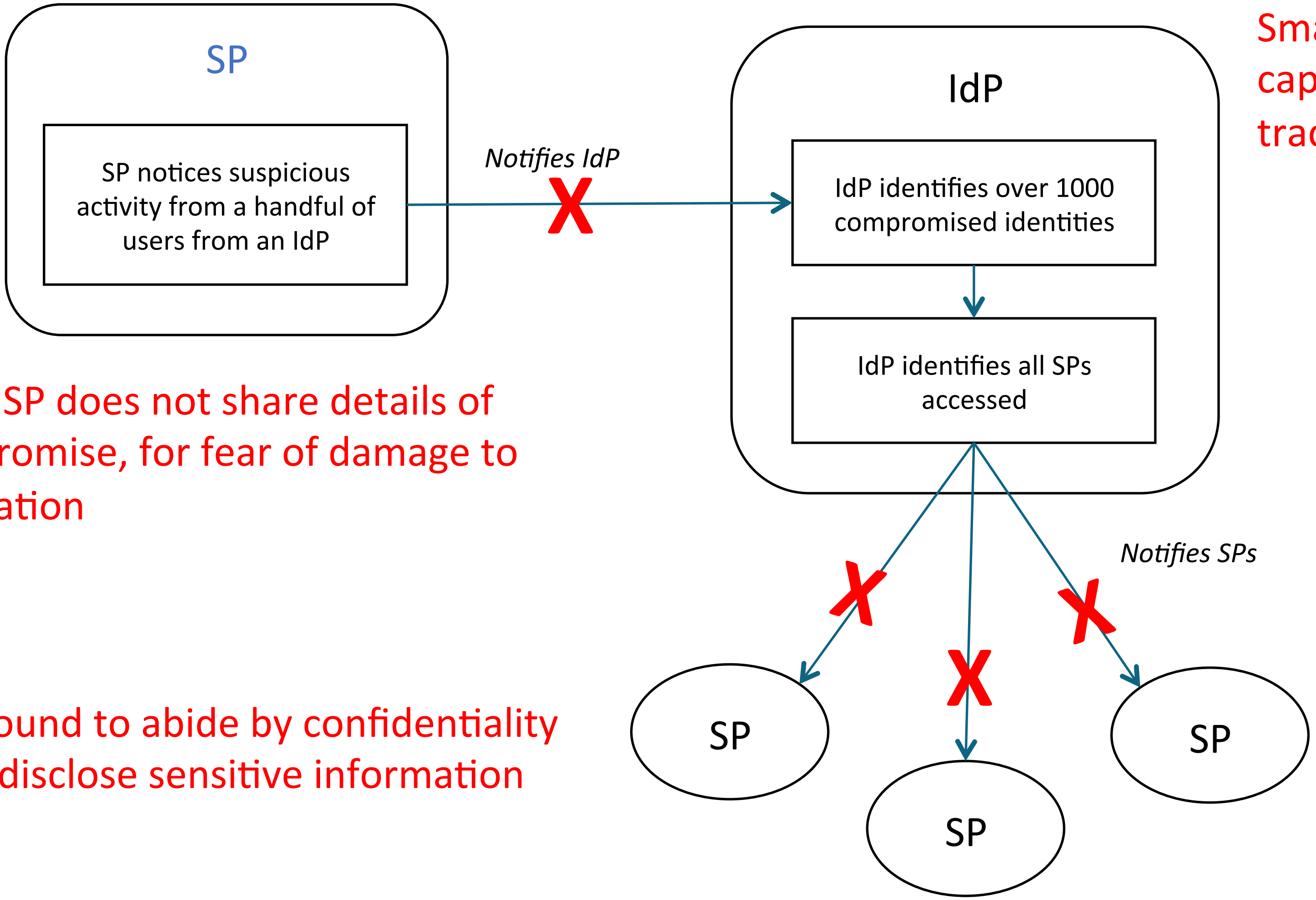
[1] https://cdsweb.cern.ch/record/1442597

It all seems like common sense…



SP
SP notices suspicious activity from a handful of users from an IdP
Notifies IdP
IdP
IdP identifies over 1000 compromised identities
IdP identifies all SPs accessed
Notifies SPs
SP
SP
SP

… but in reality


SP
SP notices suspicious activity from a handful of users from an IdP
Notifies IdP
X
IdP
IdP identifies over 1000 compromised identities
IdP identifies all SPs accessed
Notifies SPs
X
X
X
SP
SP
SP

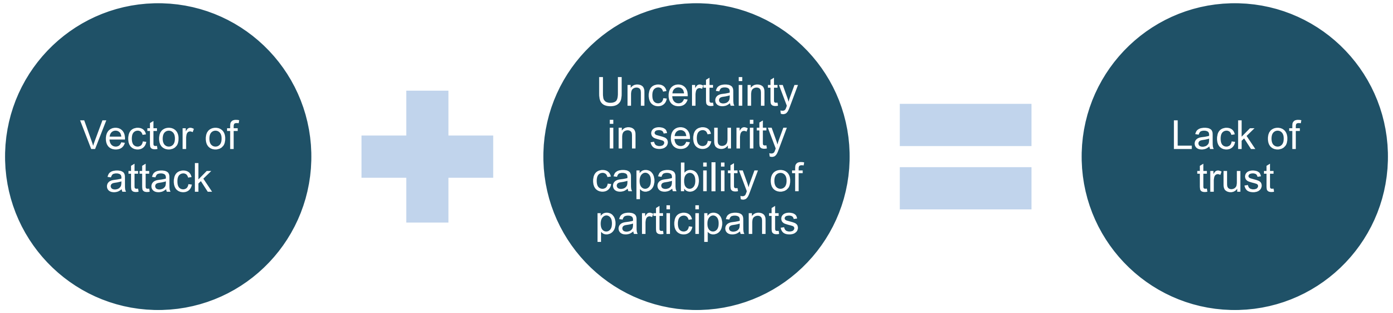
Small IdP may not have capability to block users, or trace their usage

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

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

No security contact details!

Federated Security Incident Response
The solution



Vector of attack + Uncertainty in security capability of participants = Lack of trust

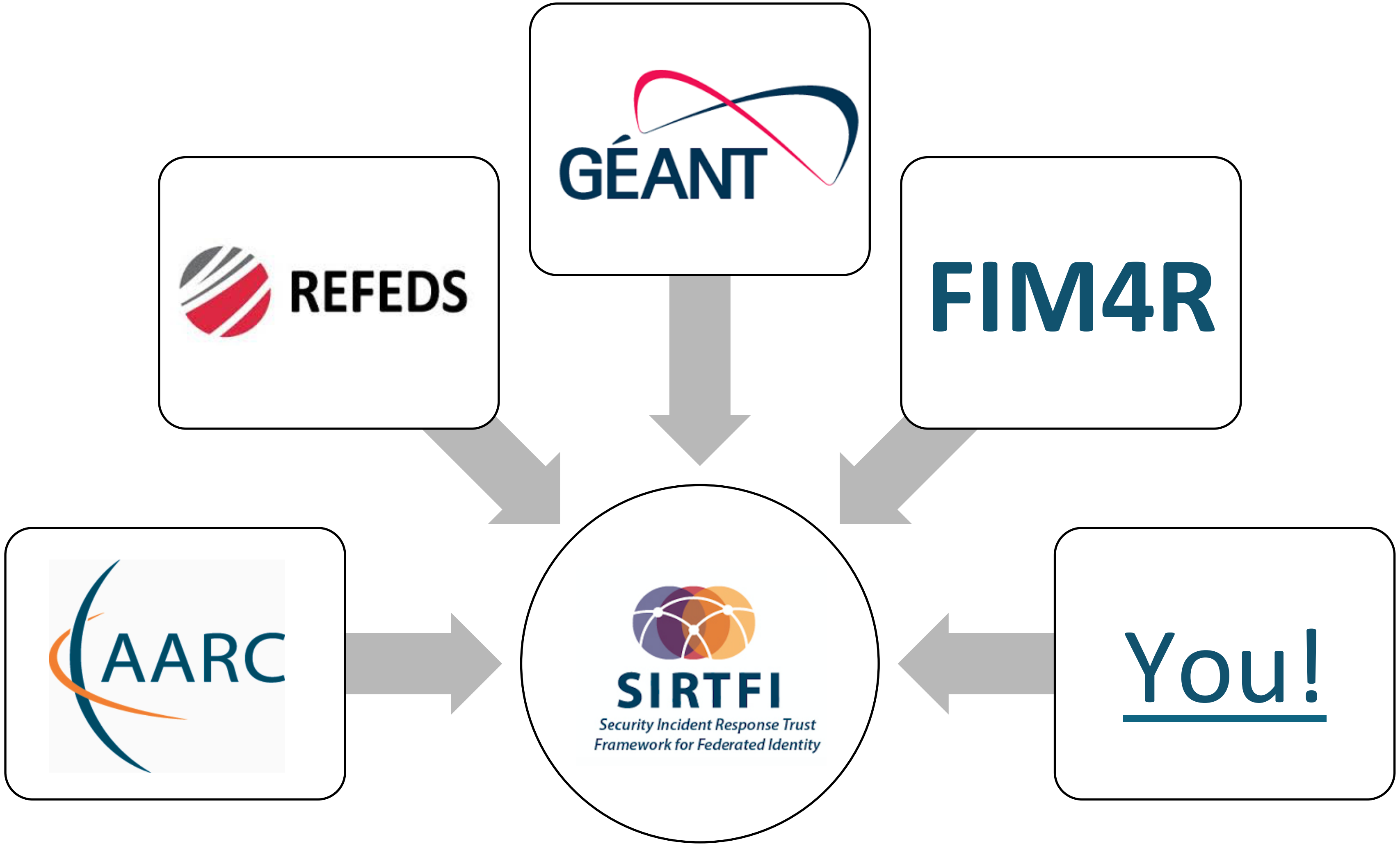
- Attacks inevitable ☹
- But we can make security capability transparent and build relationships between organisations and people ☺

…We need a trust framework!

Agenda

- Federated Security Incident Response
- What is Sirtfi?
- Why is Sirtfi important?
- What do I need to do?
- Where can I look next?

Sirtfi



REFEDS

GÉANT

FIM4R

AARC

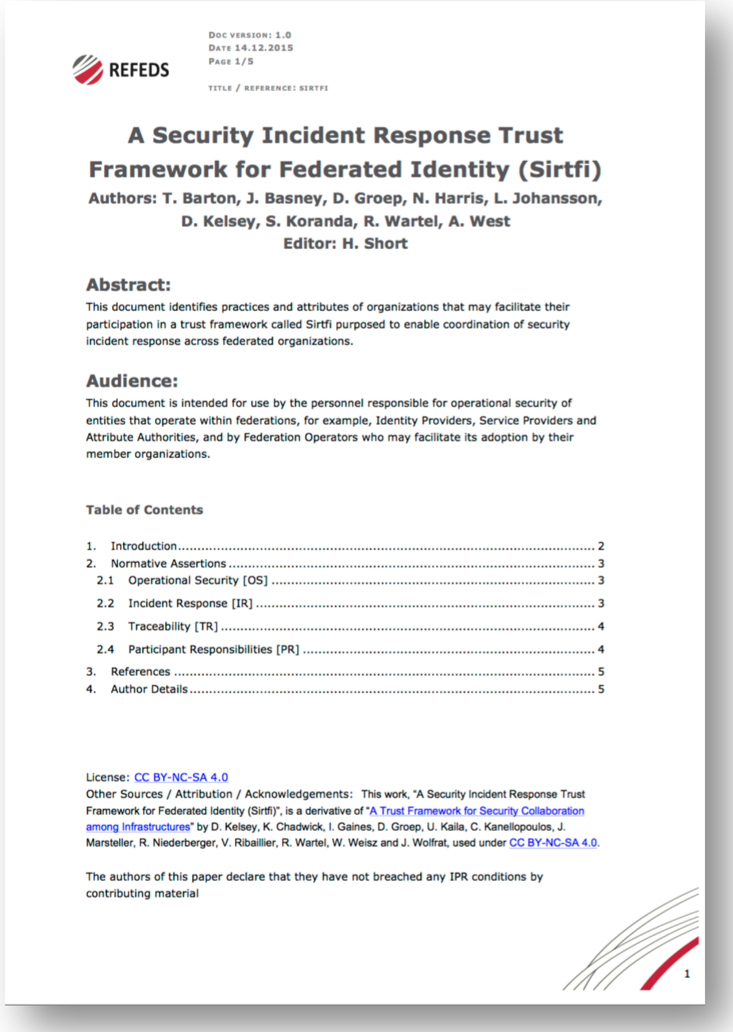
SIRTFI

Security Incident Response Trust Framework for Federated Identity

You!

Sirtfi Status

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



REFEDS

Doc version: 1.0
Date 14.12.2015
Page 1/5

TITLE / REFERENCE: SIRTFI

A Security Incident Response Trust Framework for Federated Identity (Sirtfi)

Authors: T. Barton, J. Basney, D. Groep, N. Harris, L. Johansson, D. Kelsey, S. Koranda, R. Wartel, A. West
Editor: H. Short

Abstract:

This document identifies practices and attributes of organizations that may facilitate their participation in a trust framework called Sirtfi purposed to enable coordination of security incident response across federated organizations.

Audience:

This document is intended for use by the personnel responsible for operational security of entities that operate within federations, for example, Identity Providers, Service Providers and Attribute Authorities, and by Federation Operators who may facilitate its adoption by their member organizations.

Table of Contents

Other Sources / Attribution / Acknowledgements: This work, "A Security Incident Response Trust Framework for Federated Identity (Sirtfi)", is a derivative of "A Trust Framework for Security Collaboration among Infrastructures" by D. Kelsey, K. Chadwick, I. Gaines, D. Groep, U. Kaila, C. Kanellopoulos, J. Marsteller, R. Niederberger, V. Ribaillier, R. Wartel, W. Weisz and J. Wolfrat, used under CC BY-NC-SA 4.0.

The authors of this paper declare that they have not breached any IPR conditions by contributing material

1

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 security contacts
- Guarantee a response during collaboration

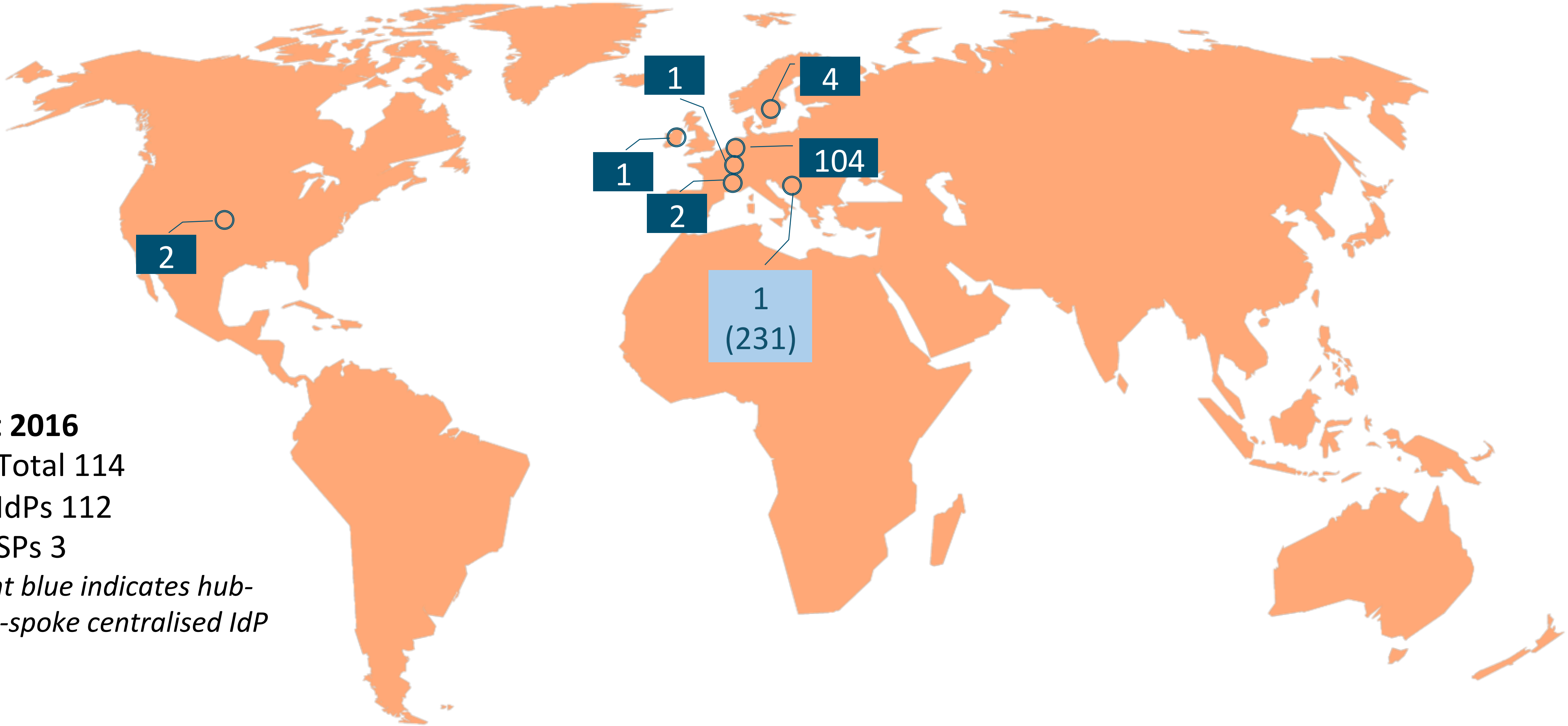
Traceability

- 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

Current Adoption



Oct 2016

- Total 114
- IdPs 112
- SPs 3

Light blue indicates hub-and-spoke centralised IdP

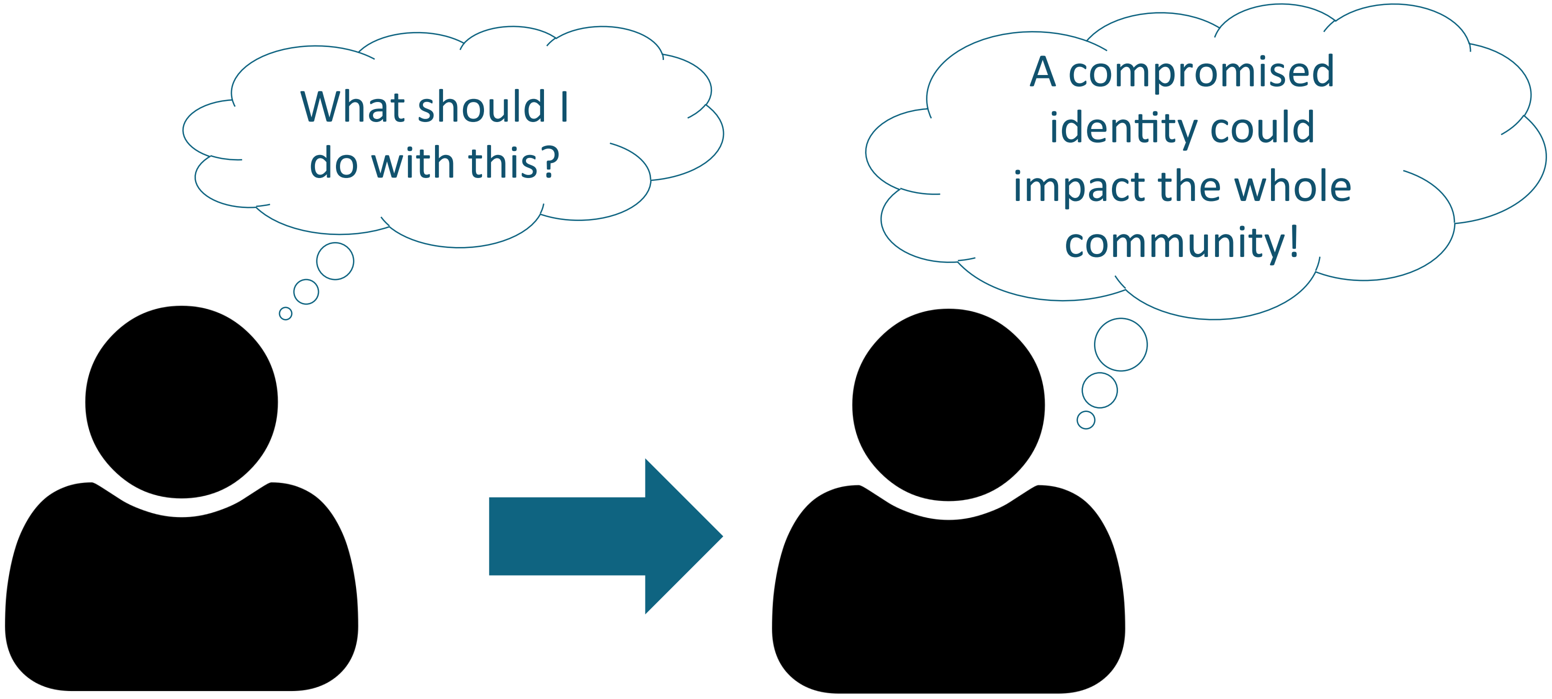
Agenda

- Federated Security Incident Response
- What is Sirtfi?
- Why is Sirtfi important?
- What do I need to do?
- Where can I look next?

Example, Credential Dump

SP admin discovers a credential dump online containing federated logins

Example, Credential Dump



What should I do with this?

A compromised identity could impact the whole community!

Discovers a credential dump online containing identities from IdPs

Considers the impact

Example, Credential Dump

What should I do with this?

A compromised identity could impact the whole community!

I should let them know…

Discovers a credential dump online containing identities from IdPs

Considers the impact

Decides to share intelligence with the community

Example, Credential Dump

What should I

A compromised
identity could

I should let
v…

By listing a security contact for your IdP, you enable intelligence sharing

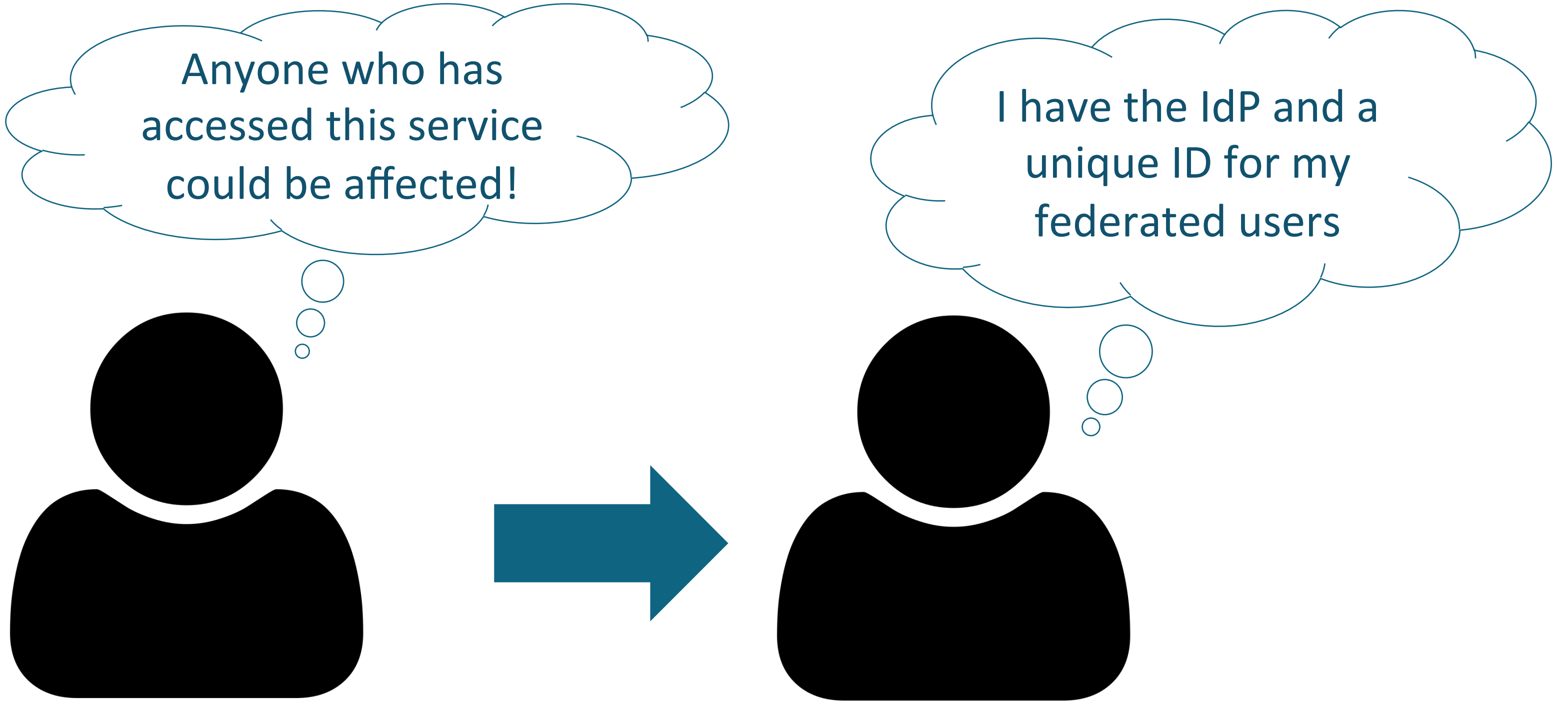
Discove
dump o
identitie

Example, Compromised Service

Anyone who has accessed this service could be affected!

Discovers that their SP has been compromised and is hosting malvertising

Example, Compromised Service



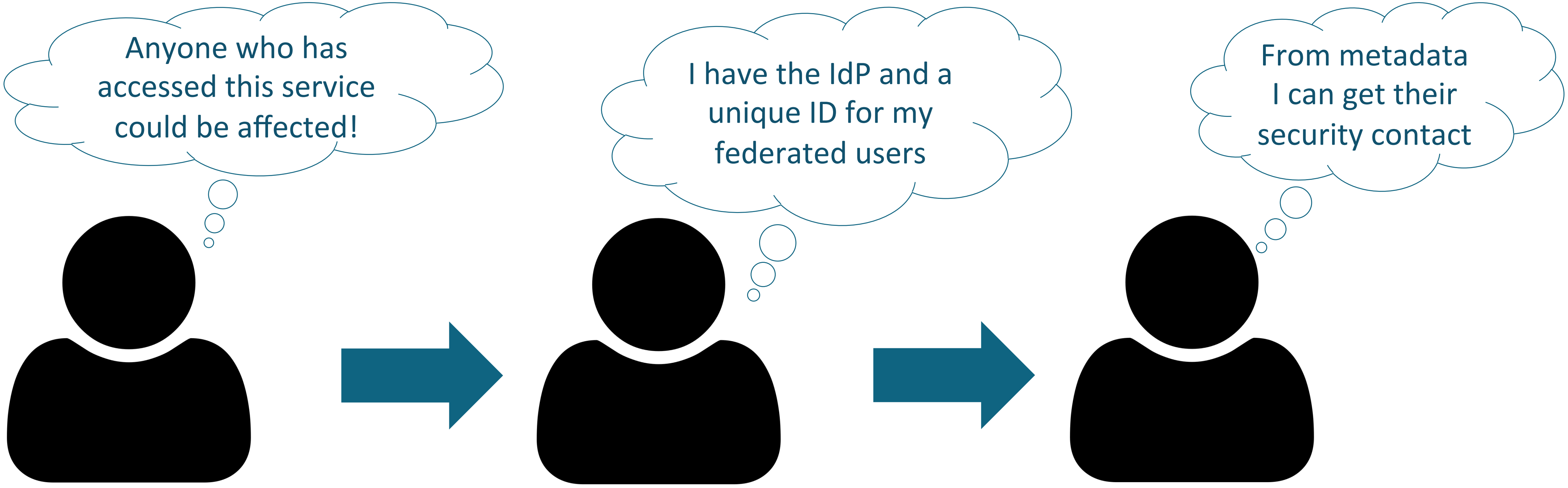
Anyone who has accessed this service could be affected!

I have the IdP and a unique ID for my federated users

Discovers that their SP has been compromised and is hosting malvertising

Identifies users that have connected

Example, Compromised Service



Anyone who has accessed this service could be affected!

I have the IdP and a unique ID for my federated users

From metadata I can get their security contact

Discovers that their SP has been compromised and is hosting malvertising

Identifies users that have connected

Informs the relevant security contact

Example, Compromised Service

Anyone who has accessed this service

I have the IdP and a

From metadata I can get their

tact

By using Sirtfi, you are part of a community working to protect R&E users

Discove

has bee

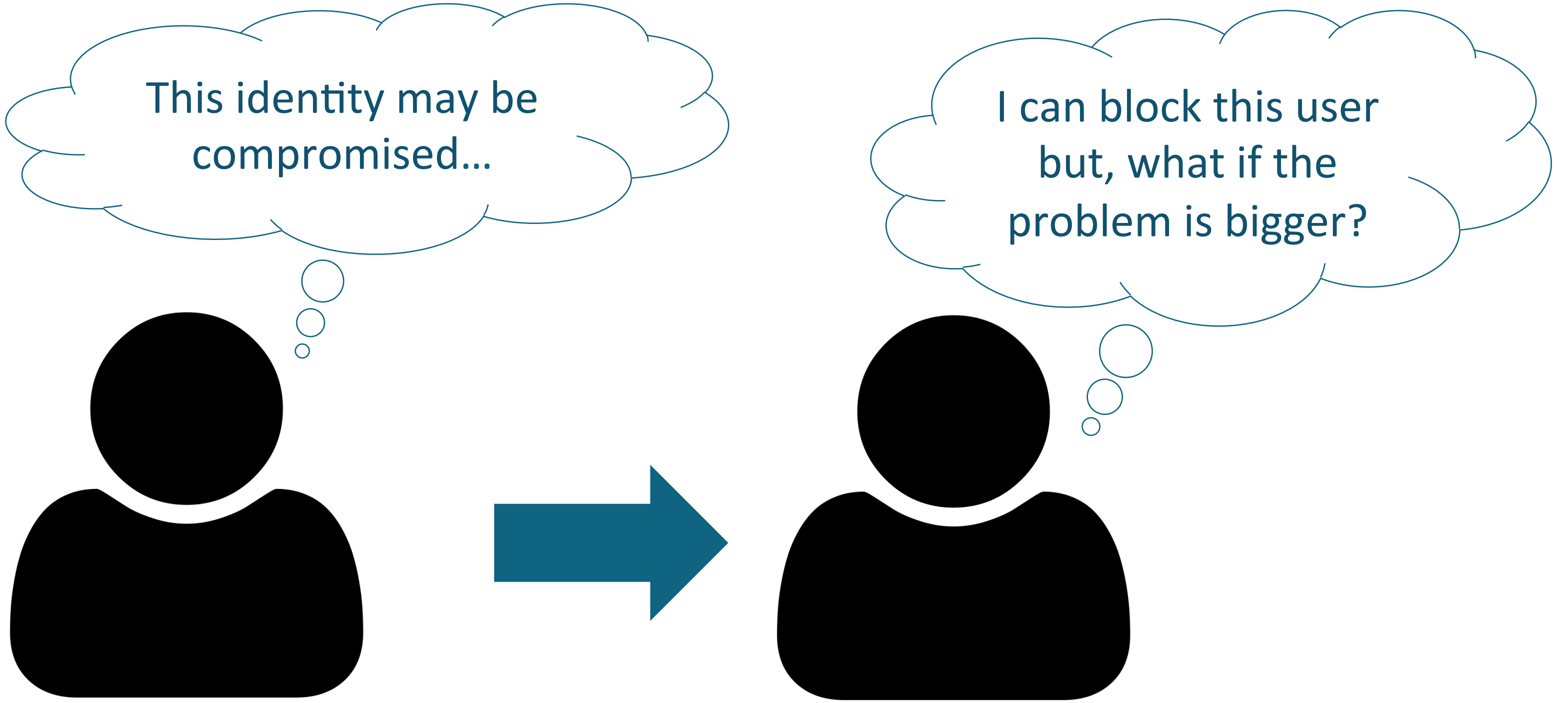
and is h

malvert

Example, Compromised Identity

Discovers suspicious file deletions at their SP, attributes this to a federated user

Example, Compromised Identity



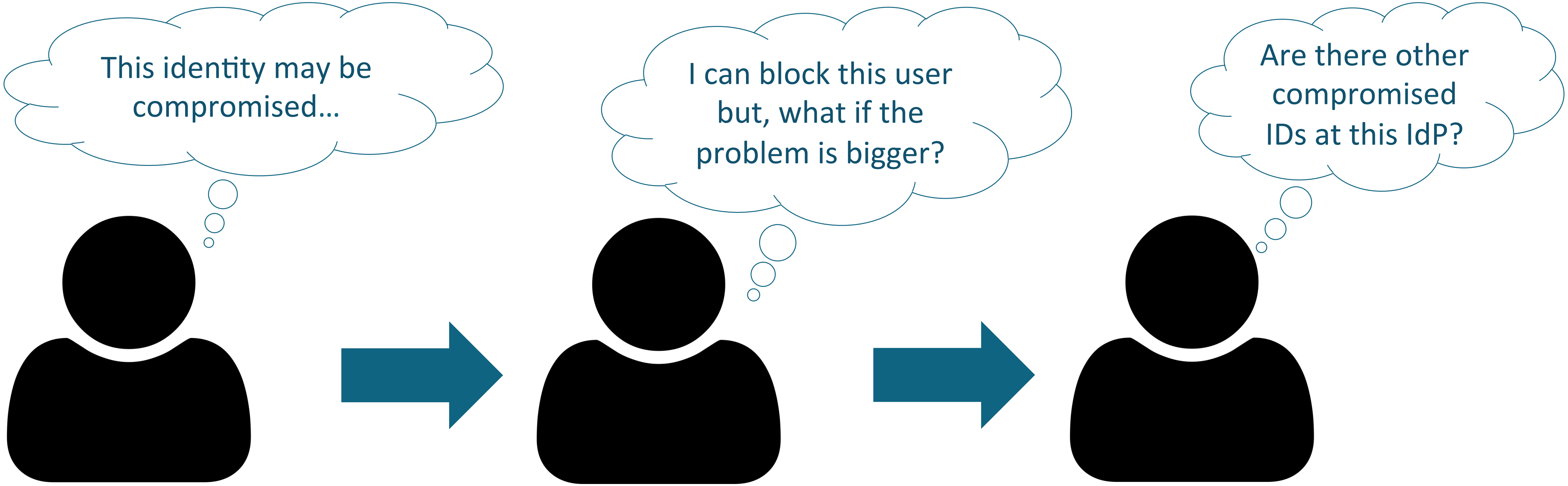
This identity may be compromised…

I can block this user but, what if the problem is bigger?

Discovers suspicious file deletions at their SP, attributes this to a federated user

Contains the situation locally

Example, Compromised Identity



This identity may be compromised…

I can block this user but, what if the problem is bigger?

Are there other compromised IDs at this IdP?

Discovers suspicious file deletions at their SP, attributes this to a federated user

Contains the situation locally

Seeks assistance from the IdP

Example, Compromised Identity

This identity may be compromised

I can block this user

Are there other compromised

dP?

As an IdP, your knowledge is essential for understanding the scope of an incident. An SP may well notice an incident before you but only you can act!

Discove
deletion
attribut
federate

Sirtfi
The benefits

IdPs
Advertise that your **users** are covered by incident response at their own organisation

SPs
Advertise that your **service** is trustworthy and covered by an incident response capability

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

Make all our systems safer together globally

Agenda

- Federated Security Incident Response
- What is Sirtfi?
- Why is Sirtfi important?
- **What do I need to do?**
- Where can I look next?

What do I need to do?

Visit the Guide for Federation Participants:
https://wiki.refeds.org/display/SIRTFI/Guide+for+Federation+Participants

Assess your security practices

- Complete a self assessment of the Sirtfi framework
- Identify a trusted security contact

Include 2 Metadata Extensions

- Sirtfi Assurance Profile
- Security Contact

This is being integrated into your resource registry

Sirtfi
Expressing compliance

- Asserting compliance via standard OASIS assurance profile specification
- Assurance profile recognised by IANA

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...>
  <md:Extensions>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
            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>
    </mdattr:EntityAttributes>
  </md:Extensions>
  ...
</md:EntityDescriptor>
```

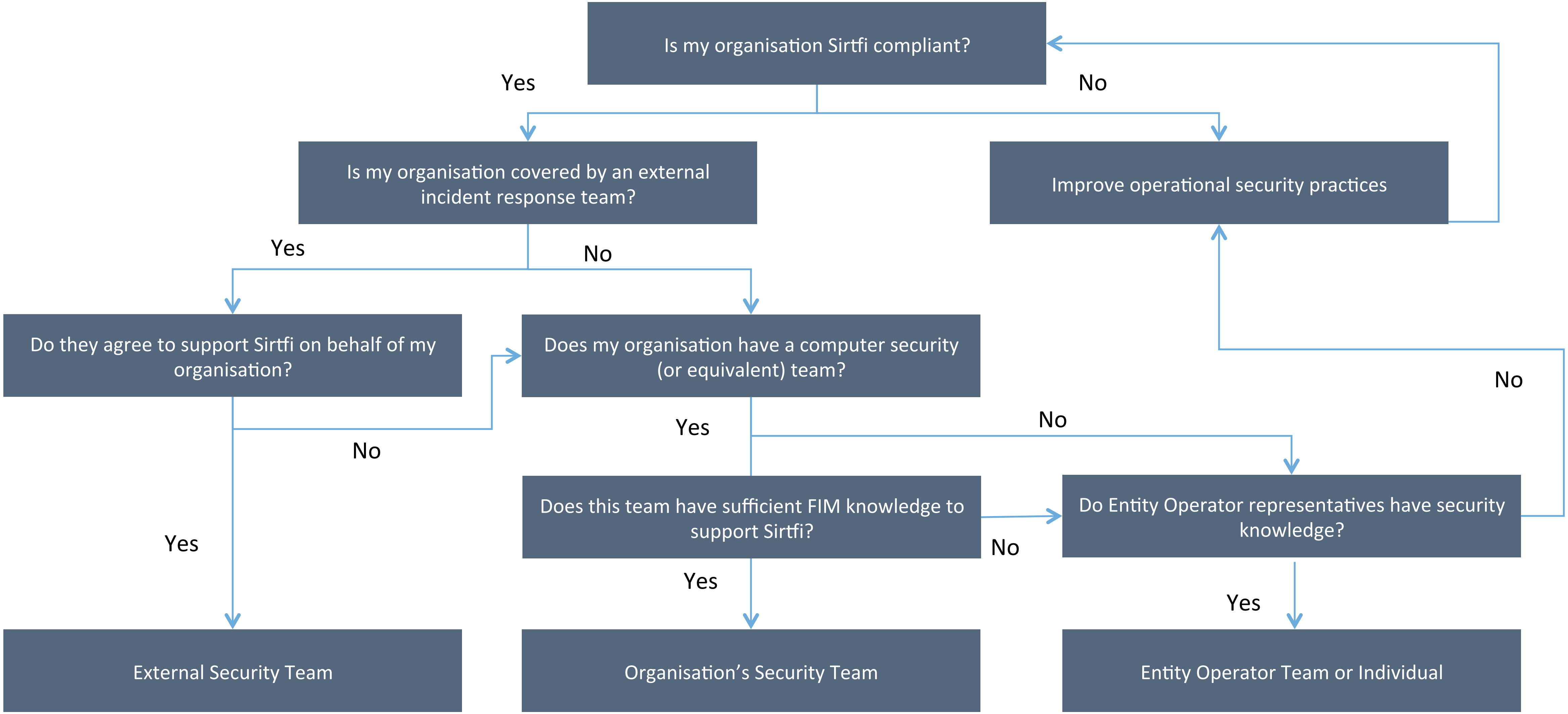
Sirtfi
Security contact expectations

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
Security contact choice


Is my organisation Sirtfi compliant?
Yes
No
Is my organisation covered by an external incident response team?
Improve operational security practices
Yes
No
Do they agree to support Sirtfi on behalf of my organisation?
Does my organisation have a computer security (or equivalent) team?
No
Yes
No
No
Yes
Does this team have sufficient FIM knowledge to support Sirtfi?
No
Do Entity Operator representatives have security knowledge?
Yes
Yes
External Security Team
Organisation’s Security Team
Entity Operator Team or Individual

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 or external teams
- What to include?
  - Mandatory GivenName and EmailAddress
  - Can add additional telephone numbers and email addresses if desired, e.g. a well known individual on a security team

```
<md:ContactPerson xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    contactType="other"
    remd:contactType="http://refeds.org/metadata/contactType/security"
    xmlns:remd="http://refeds.org/metadata">
  <md:GivenName>Security Response Team</md:GivenName>
  <md:EmailAddress>mailto:security@xxxxxxxxxxxxxx</md:EmailAddress>
</md:ContactPerson>
```

Credit to David Groep (Nikhef) for this slide

SWITCH specifics for SIRTFI

Roadmap:

- December 2016: Resource Registry update to allow Identity Providers to define security contacts and assert SIRTFI compliance
- December 2016/January 2017: Announcement to all Identity Provider administrators explaining SIRTFI and the new possibility to add it
- Q1 2017: SWITCHaai team may act as default security contact for IdP Hosting customers

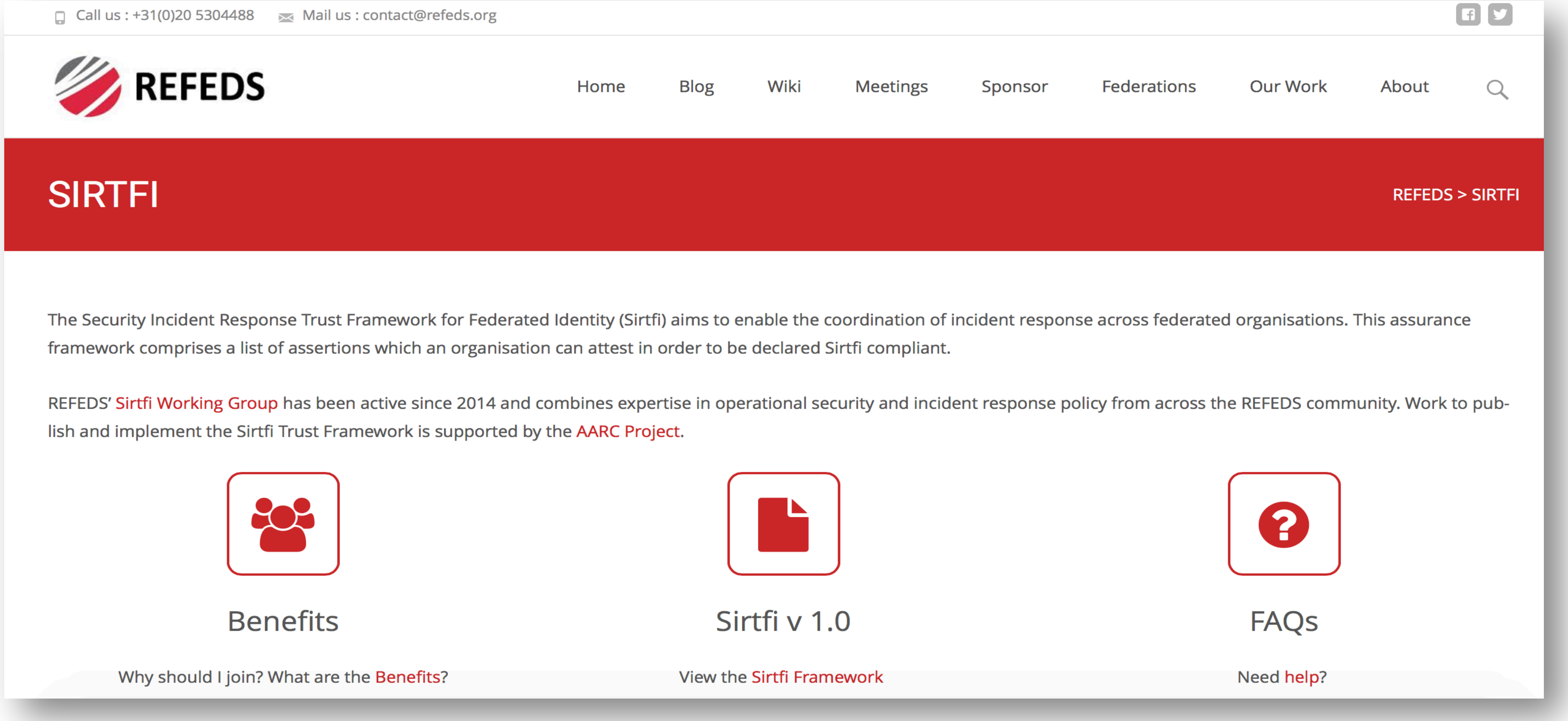
General assumptions:

- Security contacts should coordinate (or execute)
  - (a) the blocking of a compromised account and
  - (b) the following security-relevant investigations
- Effective communication between a university’s security team, their IdP admins and user directory admins is essential

Agenda

- Federated Security Incident Response
- What is Sirtfi?
- Why is Sirtfi important?
- What do I need to do?
- Where can I look next?

Sirtfi
Find out more – Home Page



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.

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 to publish 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

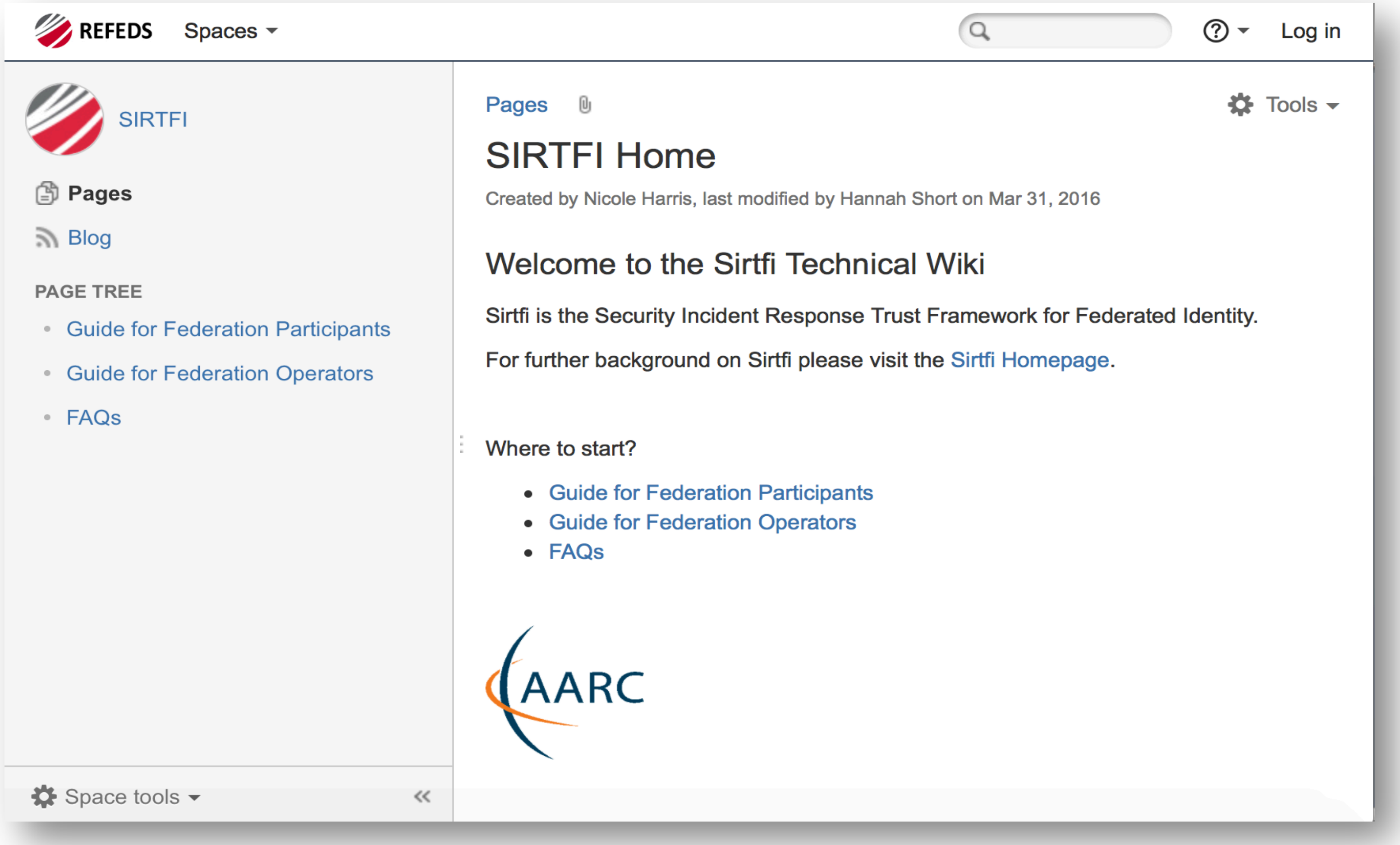
View the Sirtfi Framework

FAQs

Need help?

https://refeds.org/sirtfi

Sirtfi
Find out more – Technical Wiki



SIRTFI Home

Created by Nicole Harris, last modified by Hannah Short on Mar 31, 2016

Welcome to the Sirtfi Technical Wiki

Sirtfi is the Security Incident Response Trust Framework for Federated Identity.

For further background on Sirtfi please visit the Sirtfi Homepage.

Where to start?

- Guide for Federation Participants
- Guide for Federation Operators
- FAQs

AARC

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

Thank you

Any Questions?

hannah.short@cern.ch

AARC

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.

Thank you

Any Questions?

hannah.short@cern.ch

AARC

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).