What will the Sirtfi trust framework change for FIM4R?

Hannah Short

CERN

hannah.short@cern.ch

REFEDS, Vienna

December 1st, 2015

Background

- A Security Incident Response Trust Framework for Federated Identity

- Need for common trust framework
    - Enable coordination of security incident response
    - Vector of attack grows more inviting as magnitude of federated networks increases

- Self assertion
    - Practical compromise
    - Possible extension to peer assessment

What will Sirtfi change?

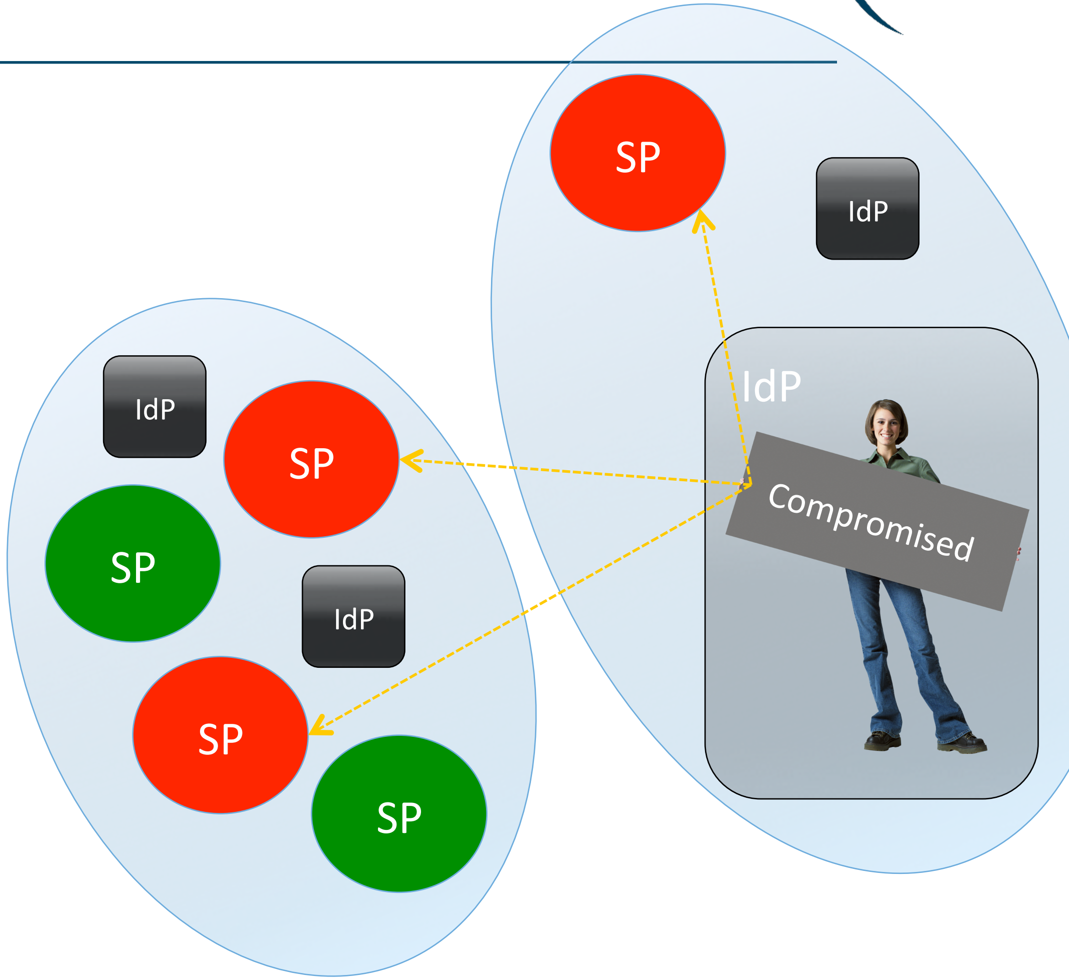
Impact on FIM4R Communities

- Trust
- Support
- Responsibility
- Self Audit

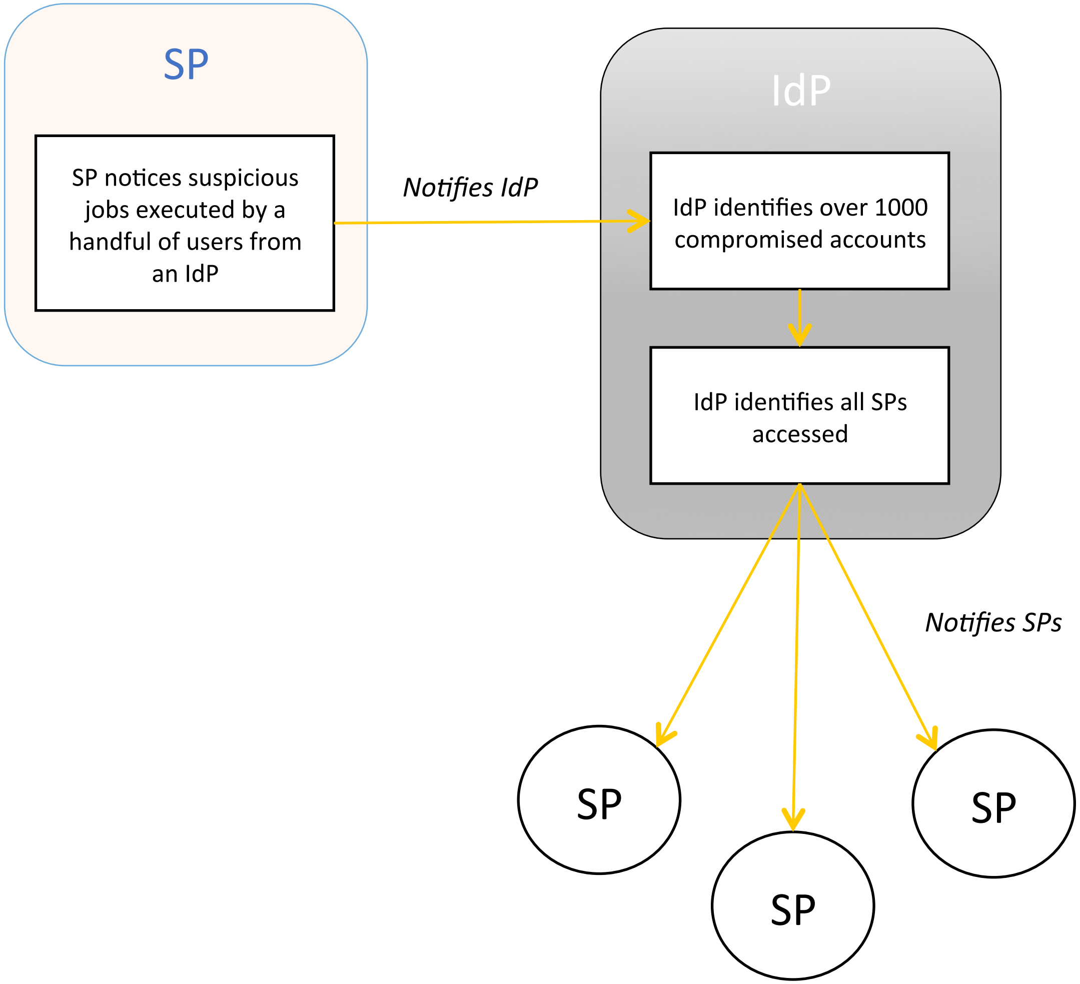
We need partners within FIM4R to pilot this framework!

Federated incidents

- Compromised account from Identity Provider (IdP) accesses external Service Providers (SPs)
- Could be **intra**-federation, or **inter**-federation
- Malicious actor is able to penetrate the network and take advantage of the lack of coordinated incident response



It all seems like common sense…



SP

SP notices suspicious jobs executed by a handful of users from an IdP

Notifies IdP

IdP

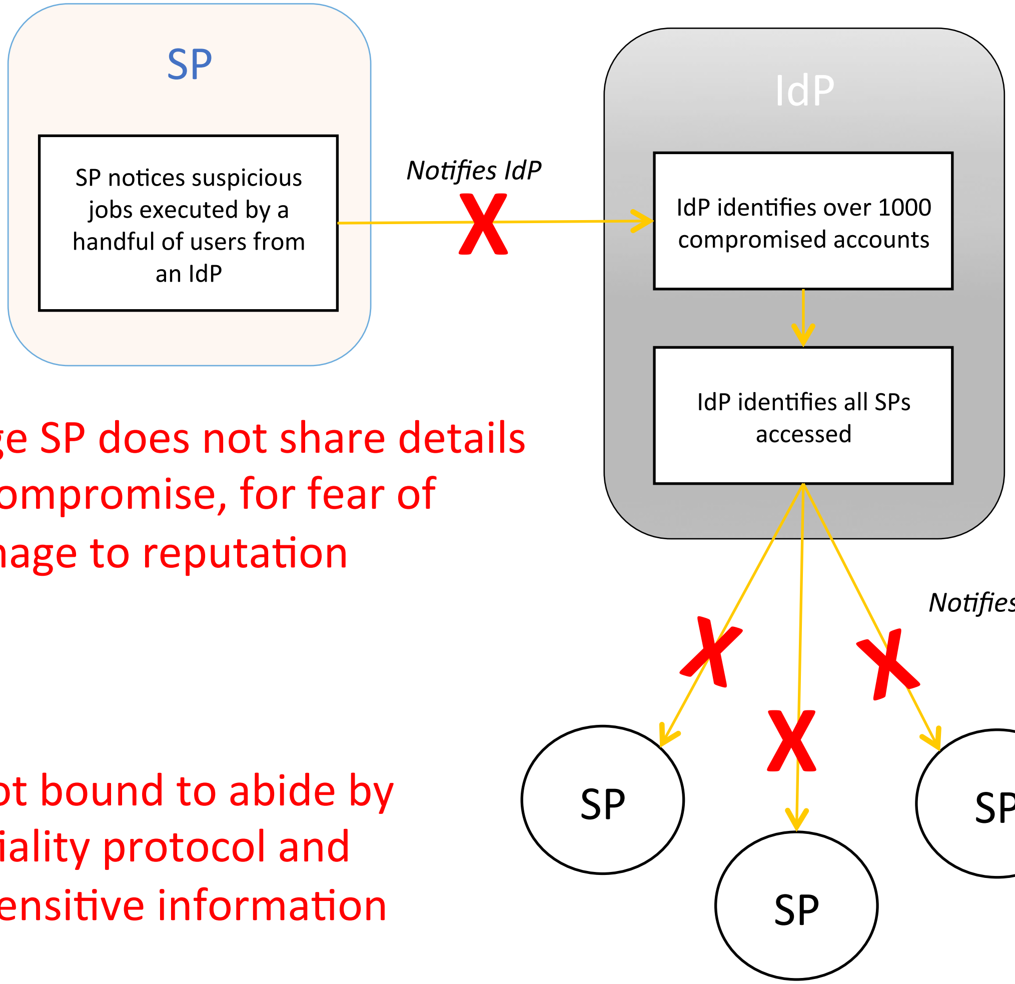
IdP identifies over 1000 compromised accounts

IdP identifies all SPs accessed

Notifies SPs

But without Sirtfi…

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


SP
SP notices suspicious jobs executed by a handful of users from an IdP
Notifies IdP
X
IdP
IdP identifies over 1000 compromised accounts
IdP identifies all SPs accessed
Notifies SPs
X
X
X
SP
SP
SP

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

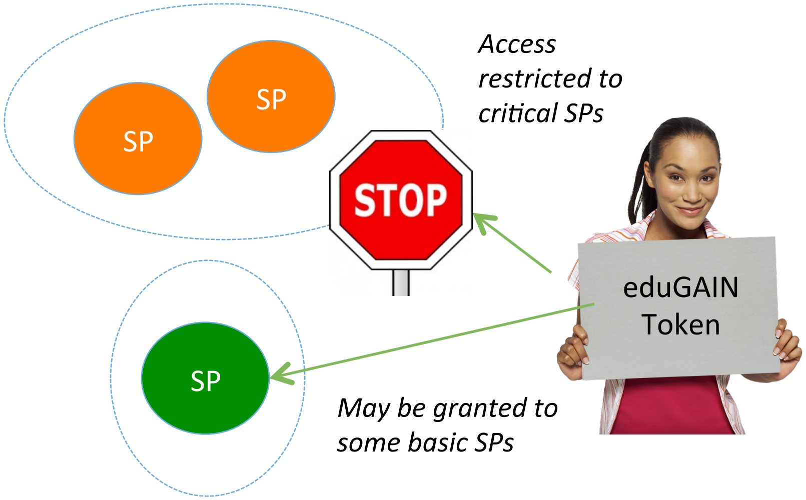
SPs are not bound to abide by confidentiality protocol and disclose sensitive information

No security contact details!

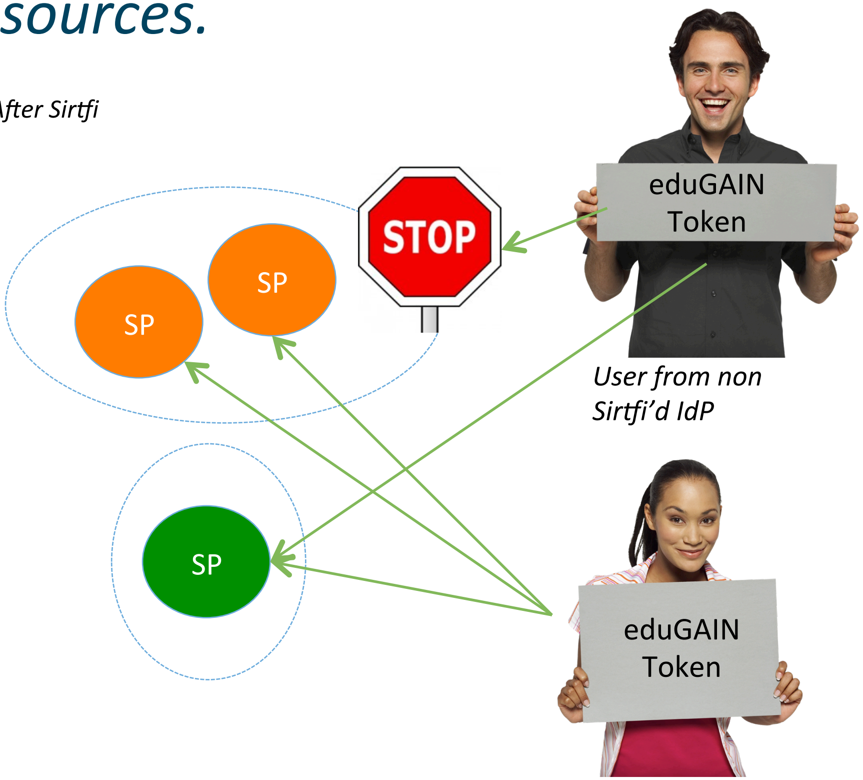
Trust

There will be a higher level of trust for Sirtfi-compliant organisations. These participants will be more likely to grant and be granted access to shared resources.

Before Sirtfi


SP
SP
STOP
SP
eduGAIN
Token
Access restricted to critical SPs
May be granted to some basic SPs

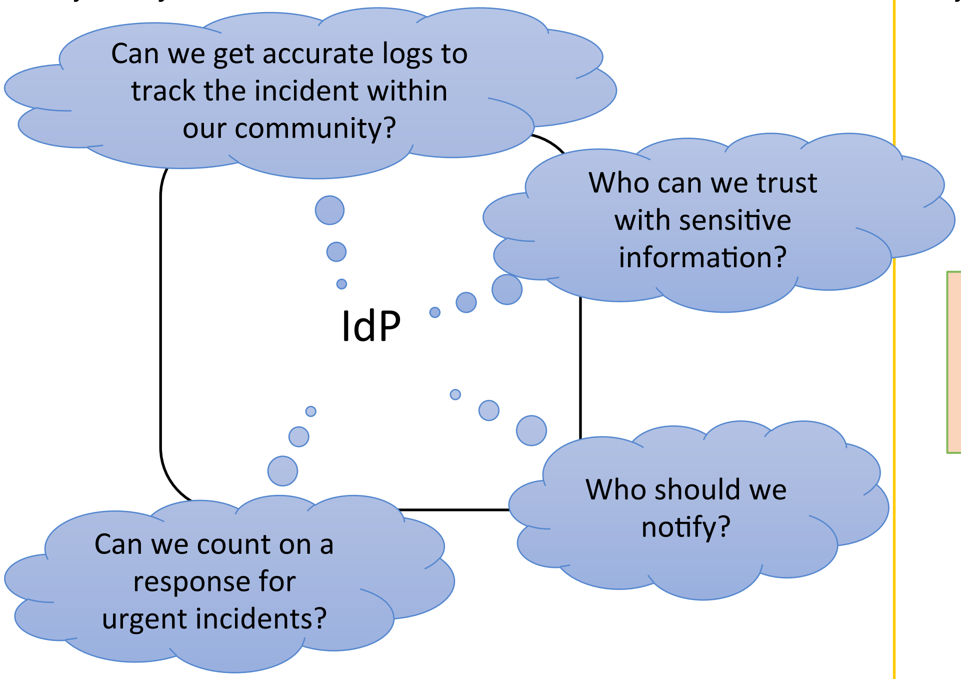
After Sirtfi



Support

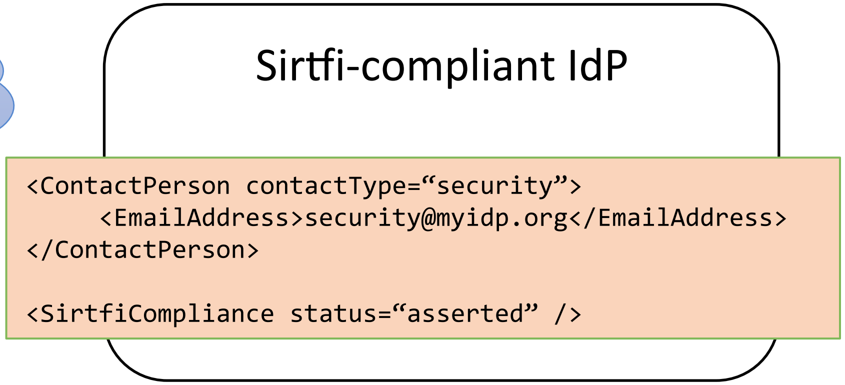
Sirtfi-compliant organisations will be able to draw on support from each other in the event of an incident. Bridging federations and identifying required expertise will be facilitated.

Before Sirtfi



Can we get accurate logs to track the incident within our community?
Who can we trust with sensitive information?
IdP
Who should we notify?
Can we count on a response for urgent incidents?

After Sirtfi



```
<ContactPerson contactType=“security”>
     <EmailAddress>security@myidp.org</EmailAddress>
</ContactPerson>

<SirtfiCompliance status=“asserted” />
```

Responsibility

Sirtfi-compliant organisations must be able to comply with support obligations in the event of a security incident. Individuals should be identified at each participating organisation and be aware of expectations.

Before Sirtfi

```
To: security@myidp.org
From: panic_stations@mysp.org

Urgent! User found submitting
malicious jobs – please investigate!
```

After Sirtfi

```
To: security@myidp.org
From: panic_stations@mysp.org

**TLP AMBER – Limited distribution
allowed **

Urgent! User found submitting malicious
jobs – please investigate! Details below…
```

```
To: panic_stations@mysp.org
Cc: security@myidp.org
From: hero@myidp.org

**TLP AMBER – Limited distribution
allowed **

Absolutely– I’m on rota this week,
account blocked and we are investigating.
Attaching relevant logs and will keep you
updated.
```

Self Audit

Sirtfi-compliant organisations will be required to complete periodic self assessments to analyse their incident response capability. Security contact information must be accurately represented in metadata and be verified during staffing and business reorganisation.

Before Sirtfi

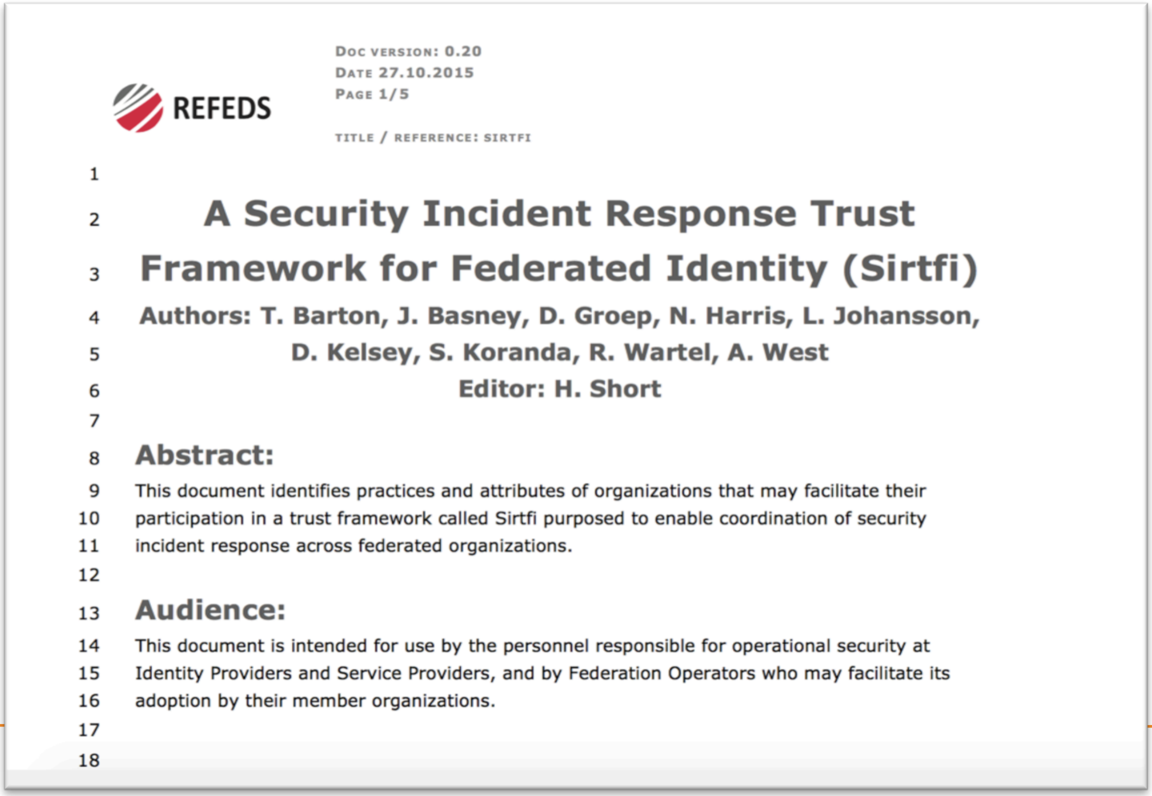
After Sirtfi

What's next?

- Potentially RFC
- LoA requirements
- Finalisation of metadata elements
  - Security contact element http://www.slideshare.net/jbasney/saml-security-contacts
  - Sirtfi compliance element
- Tool for assessing/managing Sirtfi compliance attribute
- Sirtfi v 2.0
  - Requirement to notify Sirtfi partners
  - Alerting mechanism

Sirtfi status

- Consultation closes on December 8th
- https://wiki.refeds.org/display/CON/SIRTFI+Consultation%3A+Framework
- Comments welcome!



REFEDS

DOC VERSION: 0.20
DATE 27.10.2015
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 at Identity Providers and Service Providers, and by Federation Operators who may facilitate its adoption by their member organizations.

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).