Authentication and Authorisation for Research and Collaboration

Federated Incident Response

Authentication and Authorisation for Research and Collaboration

David Groep (borrowing heavily from Hannah Short, CERN)
Policy and Best Practice activity coordination
Nikhef

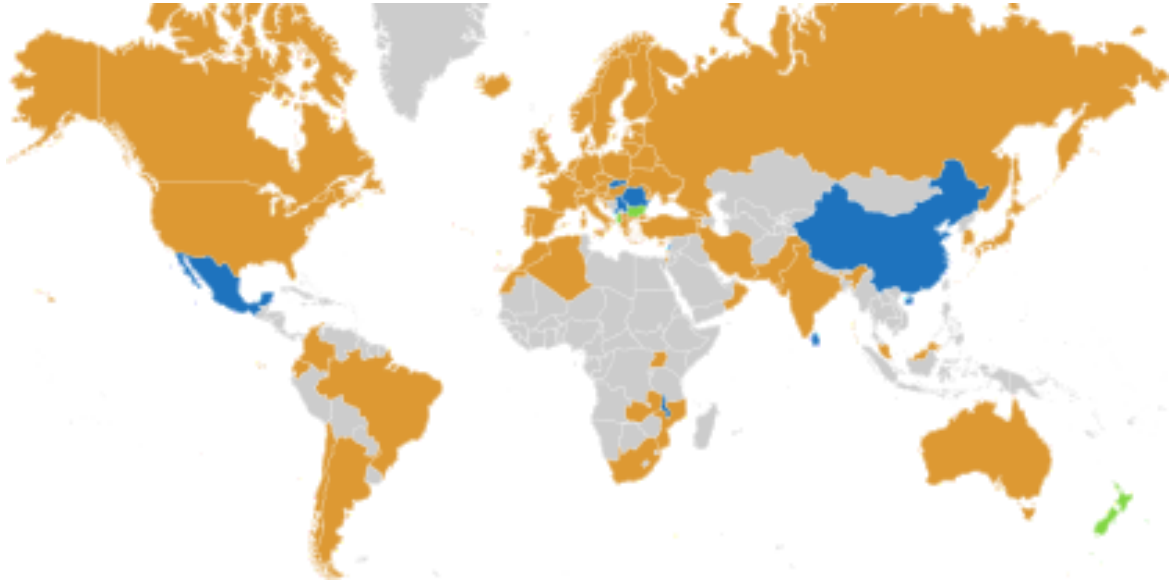
Nikhef

ISGC Security Workshop Taipei
Mach 31, 2019

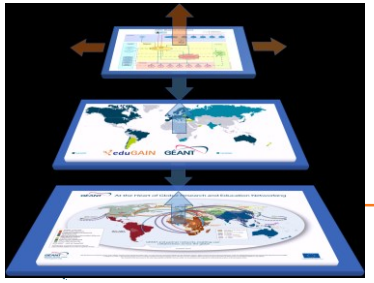
Security Workshop 2019
co-supported by EOSC-HUB

R&E federation and eduGAIN – what you may know already

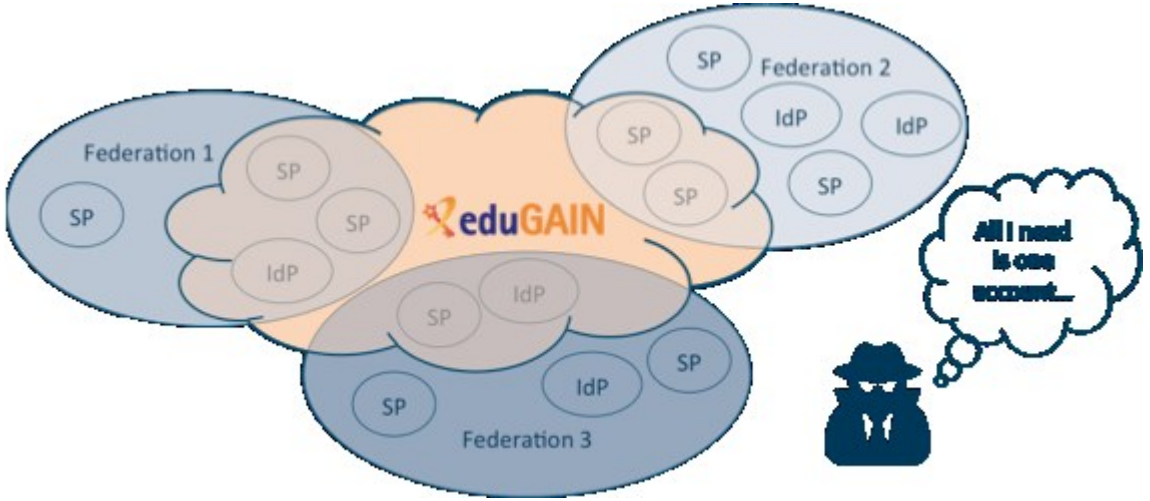
eduGAIN – many countries & economic regions with an R&E identity federation



full of valuable resources (data, network, services)

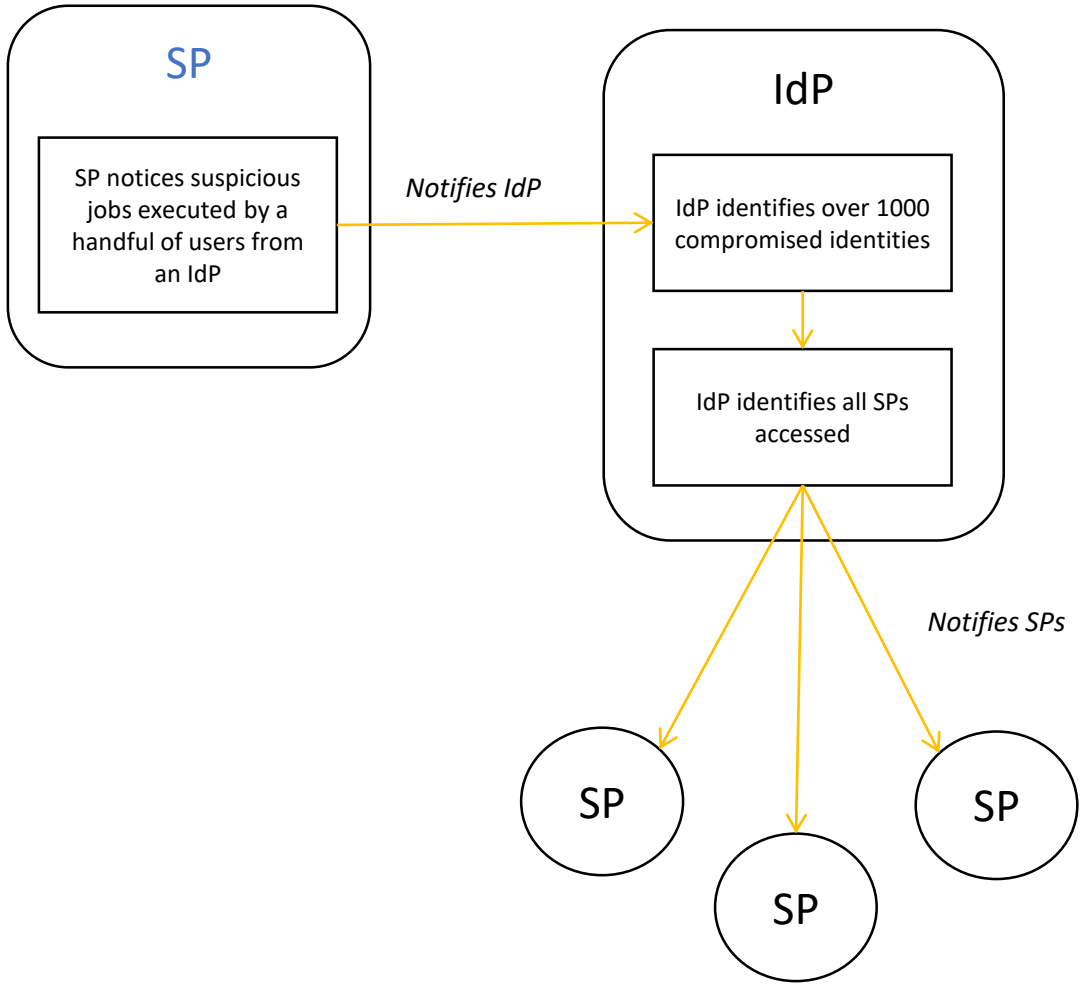


… yet incident response has to be global (since the miscreants certainly are ☹) …



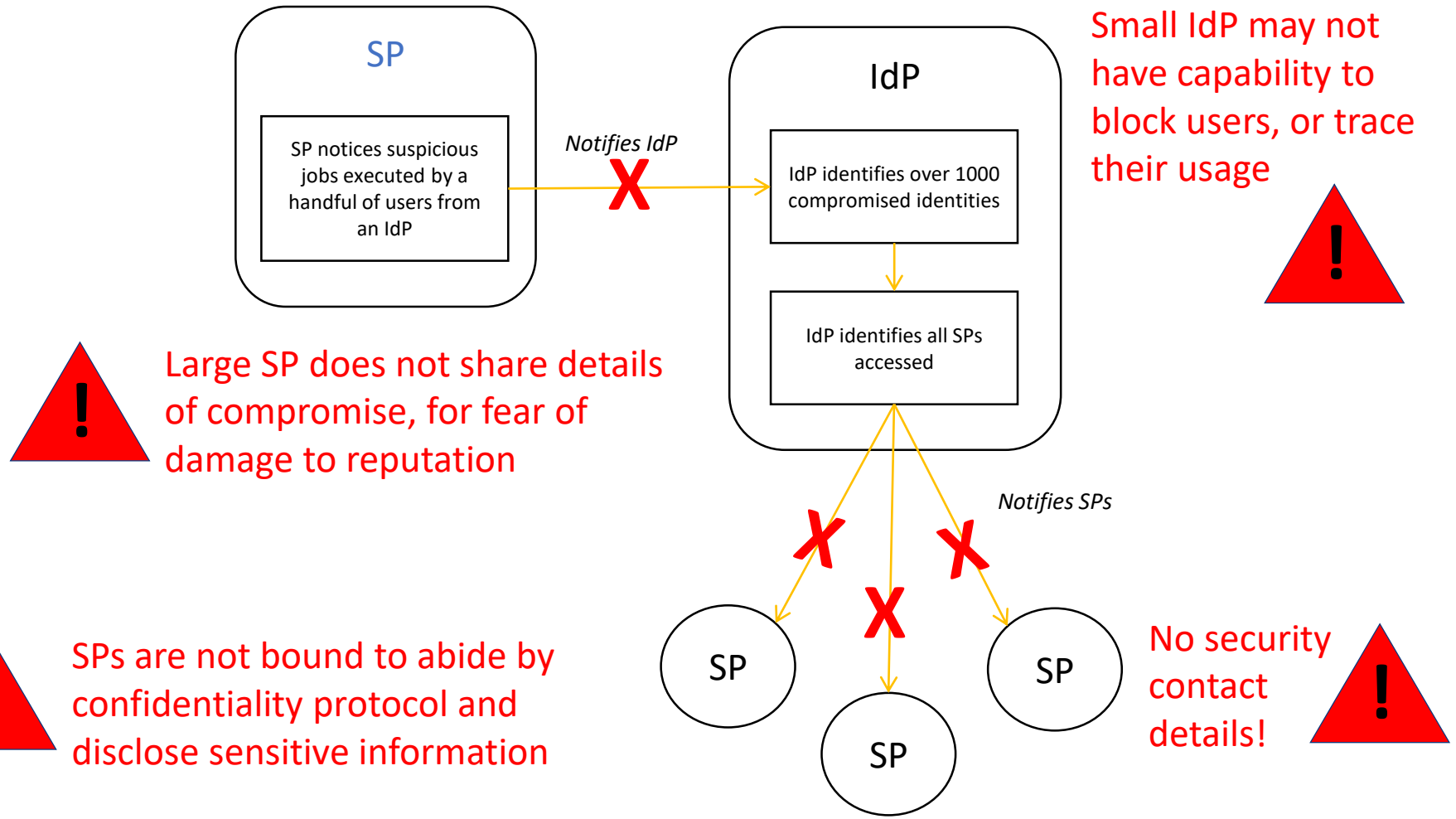
graphics sources: map technical.edugain.org; federation drawing: Hannah Short, CERN; Infrastructure logos: AARC Pilot use cases

But what appears trivial



graphics source: Hannah Short, CERN

… may not be so …



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!

graphics source: Hannah Short, CERN

A Security Incident Response Trust Framework – 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

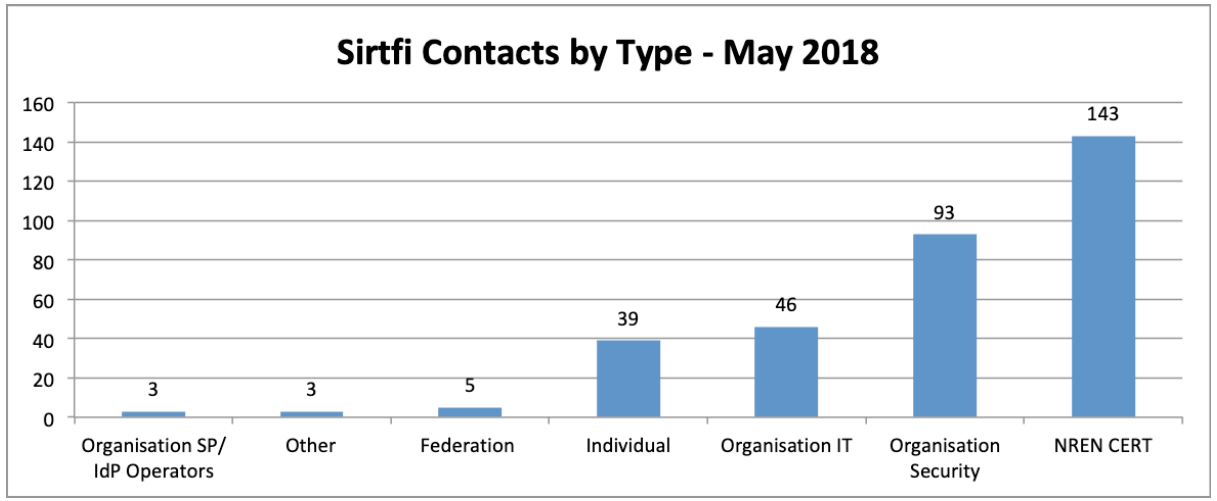
- Improve the usefulness of logs
- Ensure logs are kept in accordance with policy

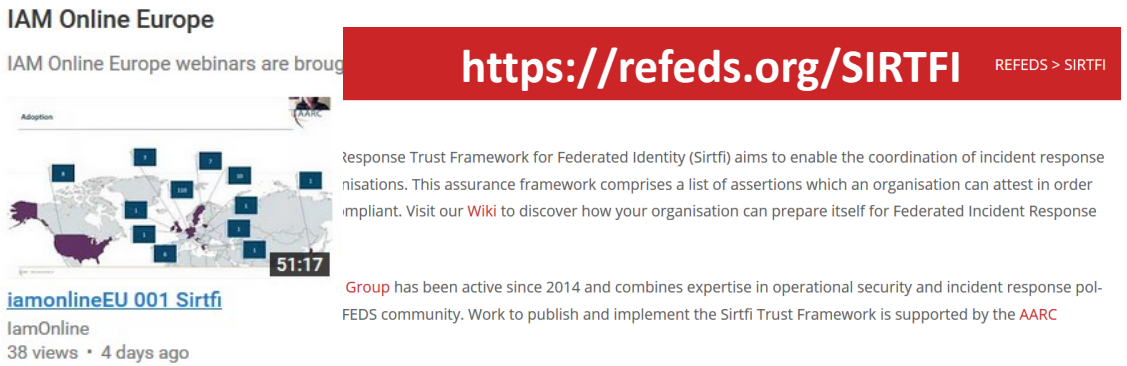
Participant Responsibilities

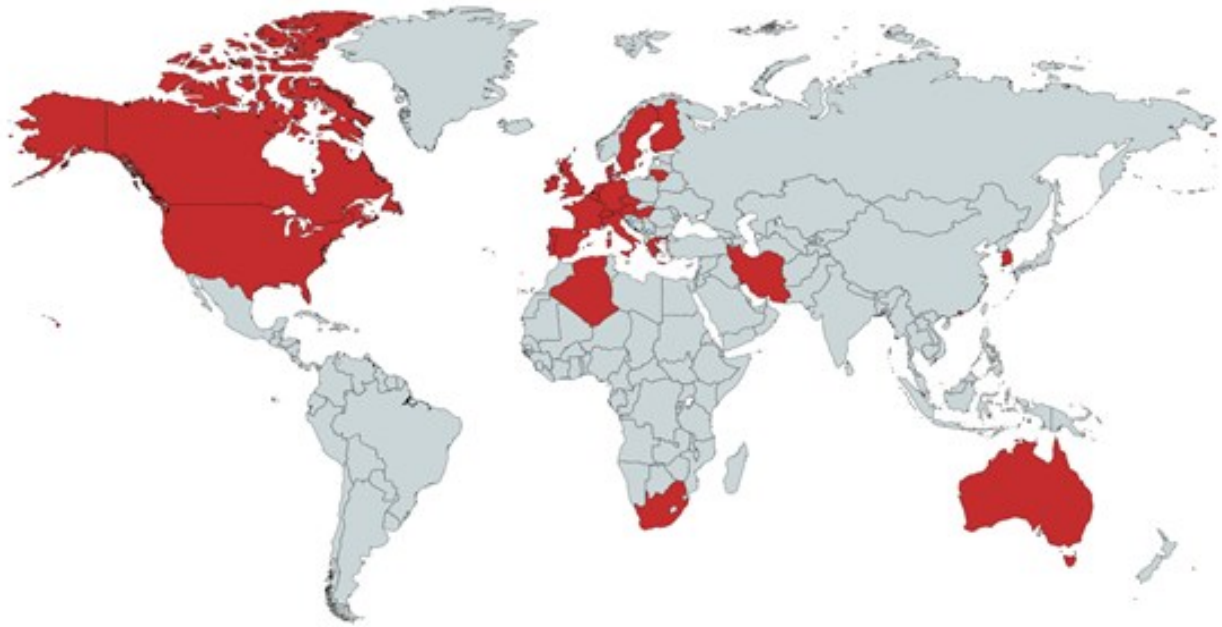
- Confirm that end users are aware of an appropriate AUP

SIRTFI
Security Incident Response Trust Framework for Federated Identity

Sirtfi today



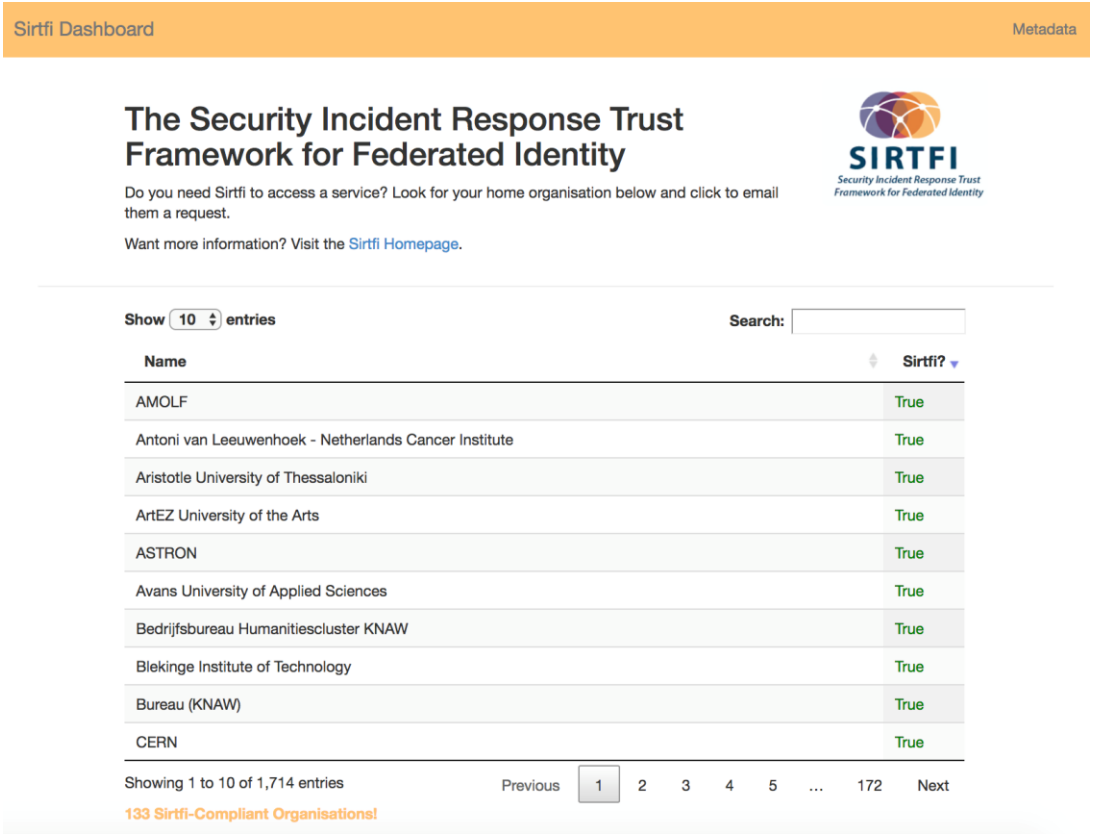




countries with at least one Sirtfi entity

graphics source: AARC2 DNA3.2 Report on Incident Response in FIM; data: technical.edugain.org

Want to check?



http://sirtfi.cern.ch/

graphics source: Hannah Short, CERN

Response: Prepare, Act, and Report

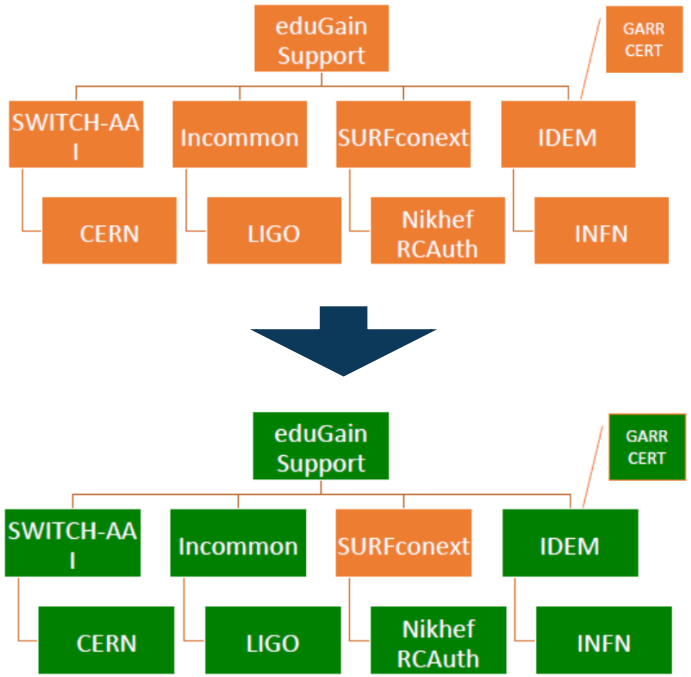
Before the incident

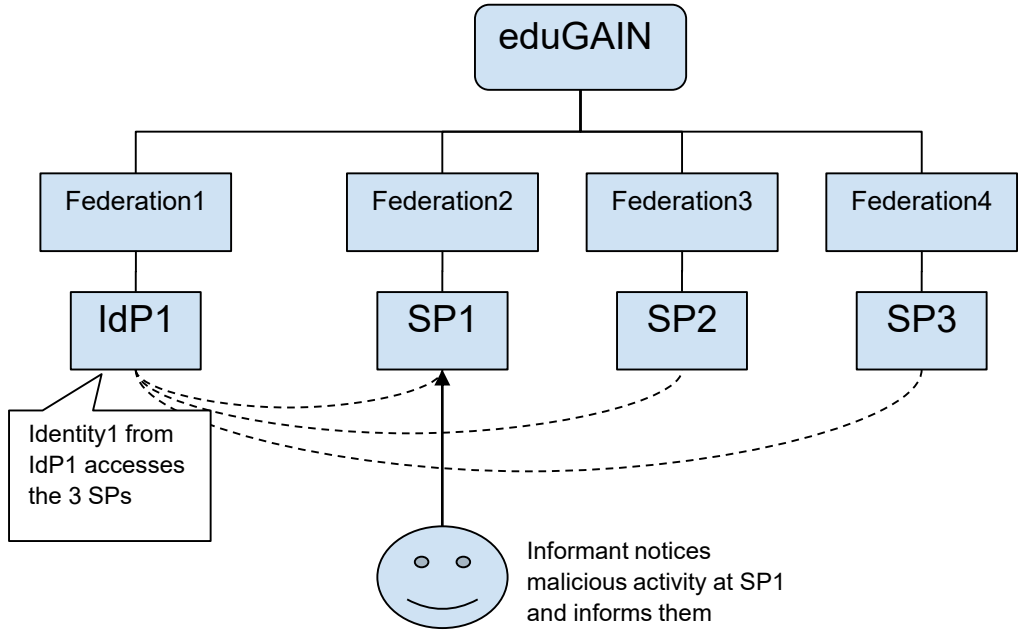
- support and implement Sirtfi – see https://refeds.org/sirtfi
- infrastructure (proxies) should adopt interoperable policies - http://wise-community.org/sci/
- identity federations should adopt common incident response procedures
  – *through the new eduGAIN support function*
- leverage templated emails to ensure proper information sharing – AARC-I051
- establish communications channels in advance

During an incident

- follow the latest procedures – from your infrastructure, federation, eduGAIN, or (NREN) CERT
- initial procedures available at https://aarc-project.eu/guidelines/aarc-i051/
- https://wiki.geant.org/display/AARC/Operational+Security+and+Incident+Response

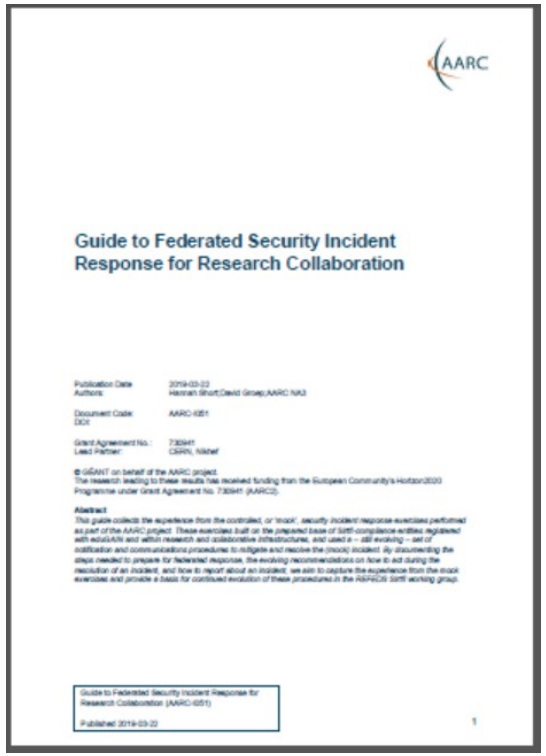
Exercising the processes with mock incidents





Exercise date	Report	URL
March 2018	Incident Simulation #1 Report	https://aarc-project.eu/wp-content/uploads/2018/04/20180326-Incident-Simulation-Report.pdf
November 2018	Incident Simulation #2 Report	https://aarc-project.eu/wp-content/uploads/2018/11/Incident-Response-Test-Model-for-Organisations-Simulation-2.pdf

AARC-I051 – the current best practice (and evolution)



Guide to Federated Security Incident Response for Research Collaboration

How to be effective during an incident?

3.4. *Roles and Responsibilities*

3.4.1. Roles and Responsibilities of Federation Participants

- Follow the [OS], [IR], [TR], and [PR] requirements described by Sirtfi [1]
- Publish valid security contact information in federation metadata as defined by the REFEDS Security Contact Schema [2]
- Report all security incidents posing a risk to any other federation participant within or outside their own federation, to the federation security contact point at their own federation

3.4.2. Roles and Responsibilities of Federations

- Follow the [IR] requirements described by Sirtfi, and [OS], [TR] and [PR] as applicable [1]
- Provide a security contact point (e.g. security@federation.org) available to all federation participants, federation operators, other federations and external organisations
- Define communication channels to be used for security incident response by federation participants

3.5. *Procedures*

3.5.1. Security Incident Response Procedure for Federation Participants

1. Follow security incident response procedures established for the organisation.
2. Contain the security incident to avoid further propagation whilst aiming at carefully preserving evidence and logs. Record all actions taken, along with an accurate timestamp.
3. Report the security incident to their federation security contact point within one local working day of the initial discovery or notification of the security incident.
4. In collaboration with the Federation Security Incident Response Coordinator, ensure all affected participants in the federation (and, if applicable, in other federations), are notified with a "heads-up" and can take action.
5. Announce suspension of service (if applicable) in accordance with federation and interfederation practices.
6. Perform appropriate investigation, system analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. Identifying the cause of security incidents is essential to prevent them from reoccurring. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected participants.
7. Share additional information as often as necessary to keep all affected participants up-to-date with the status of the security incident and enable them to investigate and take action should new information appear.
8. Respond to requests for assistance from other participants involved in the security incident within one working day.
9. Take corrective action, restore access to service (if applicable) and legitimate user access.
10. In collaboration with the Federation Security Incident Response Coordinator, produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labelled TLP AMBER [3] or higher.
11. Update documentation and procedures as necessary.

Besides the basic 'heads-up' notification template provided here, additional templates might be available within your federation or Infrastructure – refer to your federation incident response information pages or the Sirtfi web site.

The names of the organisations used below are for example purposes only.

```
Subject: [CERNCERT-2016-12-24] HEADS-UP: Multiple identities compromised at
 Acme Corporation [TLP:AMBER]

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Dear affected eduGAIN participants,

TLP:AMBER

## SUMMARY ##

The CERN CERT has detected multiple identities being compromised at the
Acme Corporation IdP. CERN is investigating the case and has reported the
abuse to Acme Corporation (no reply yet).
Early forensics findings highlighted several eduGAIN participants (all
recipients of this email) are likely affected and should urgently check
their security status.

This is an ongoing investigation and more details will be shared as they
become available.

## INTRUSION TIMELINE ##

2016-12-24 06:01: Will. E sends an abuse complaint to the CERN CERT.
```


AARC-I051 – https://aarc-project.eu/guidelines/aarc-i051/

Summary and what to do today (OK: and also tomorrow …)

Prepare

- support and implement Sirtfi - https://refeds.org/sirtfi
- adopt interoperable policies - http://wise-community.org/sci/
- adopt common incident response procedures – AARC-I051
- leverage templated emails for proper information sharing
- establish communications channels in advance

and be plugged-in … **share**, with the support of your infrastructure CERT/CSIRT teams

- Access to security contacts
- Access to threat intelligence
- Access to vulnerability reports
- Access to expertise for advanced incident investigation, e.g. forensics
- Fostering of trust between members

Trusted Introducer

eduGAIN security

nren-CERT

EGI-CSIRT

REN-ISAC

FIRST

Planned progress on “SCC Coordination”

- More exercises, coordinated via WISE
- Improve available tooling
- Promote sharing of trust resulting from exercises

Thank you

Any Questions?

davidg@nikhef.nl

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 Agre

Shameless plug: WISE & SIGISM Kaunas meeting

WISE Community: Security Communication Challenges Coordination WG (SCCC-WG)

Introduction and background

Maintaining trust between different infrastructures and domains depends largely on predictable responses by all parties involved. Many frameworks – e.g. SCI and Sirtfi – and groups such as the coordinated e-Infrastructures, the IGTF, and REFEDS, all promote mechanisms to publish security contact information, and have either explicit or implicit expectations on their remit, responsiveness,

https://wise-community.org/events/

https://eventr.geant.org/events/3044