AARC Authentication and Authorisation for Research and Collaboration

Raising Security and Trust in our Inter-Federated World

Hannah Short

IT-DI-CSO

CERN

ISGC, Taipei

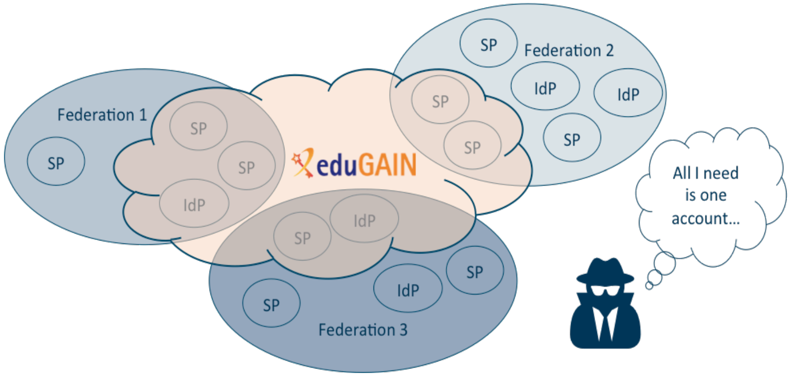
12-18 March, 2016

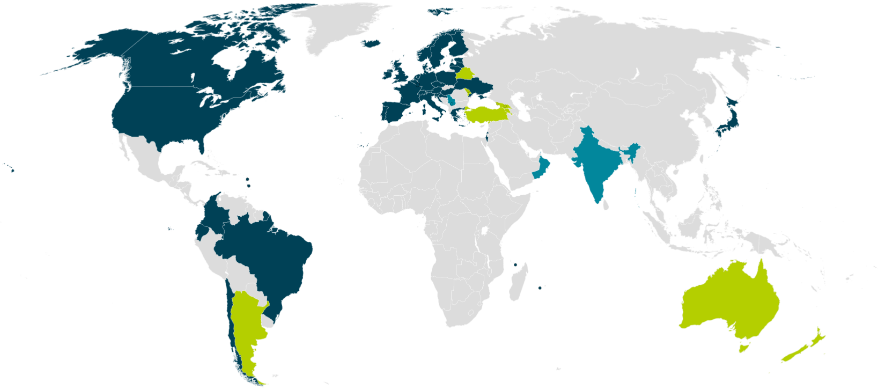
Agenda

- The federated landscape
- Common vectors of attack
- Incident response
- Building trust between organisations
- Building trust between individuals

The federated landscape

61 national federations





40 federations in eduGAIN

The federated landscape

- National Identity Federations are groups of geographically bound organisations that agree to work together
- Each Federation has its own policy set for all participants
- EduGAIN links these federations together – interfederation – and has a further policy set

There is no interfederation helpdesk

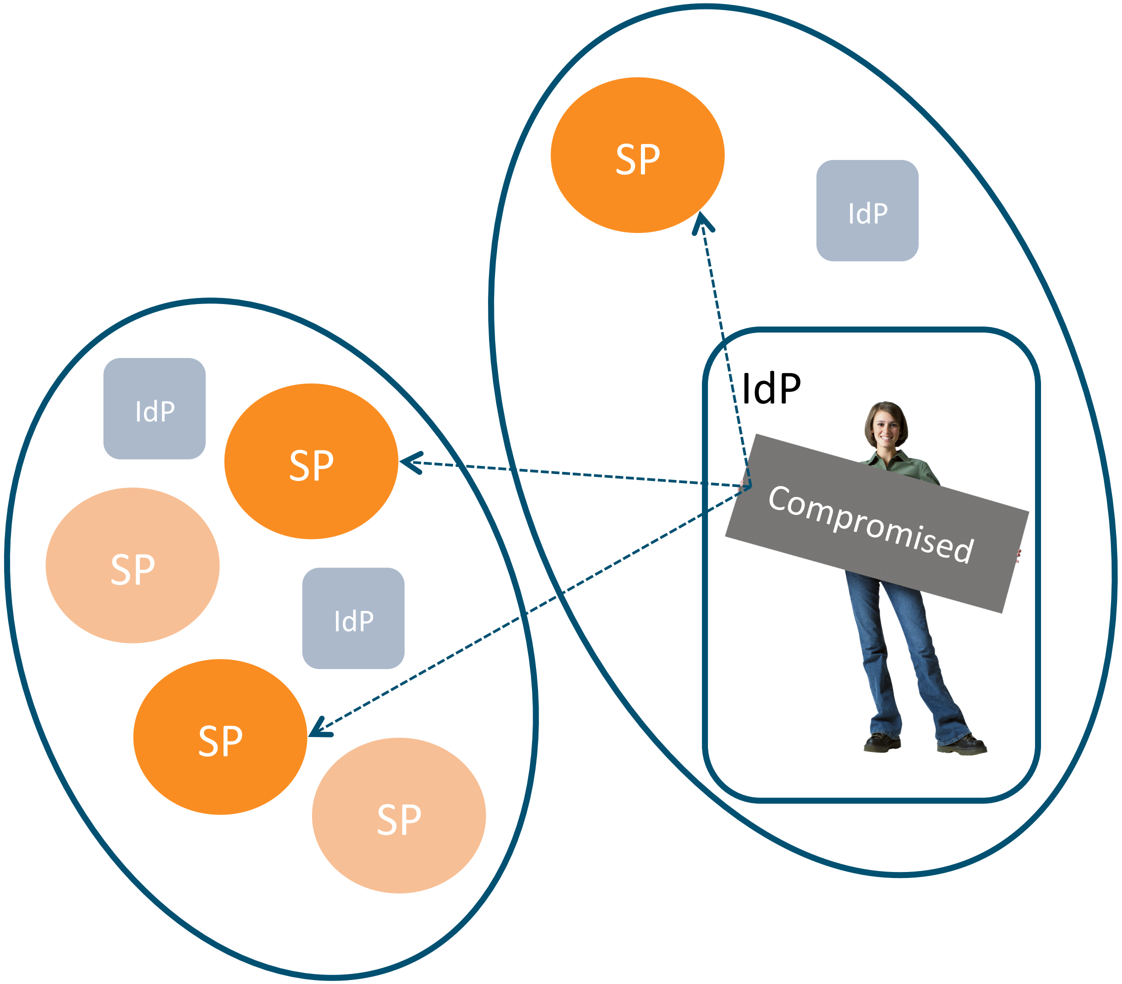
Opt-In model requires confidence in other entities

Shared policies do not automatically equal trust

https://www.switch.ch/aai/support/presentations/crash-course-2013/InterFed_all_slides.pdf

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



Common vectors of attack

Interpol: Cyber-crime is bigger than cocaine, heroin and marijuana trafficking put together

Cyber-crime is easier than ever

- Malware as a service
- Outsourcing to allow plausible deniability
- Mature, complex frameworks have been developed over many years

Typical features

- Custom 0-days, targeted phishing
- Target end-users, administrators and organisations, GoZ, Dridex, etc.
- Large distributed malicious infrastructure

Why does this affect Research and Education?

Most of our data is public, plus we have little money… why would someone go to all that trouble?

Common known objectives of intrusions

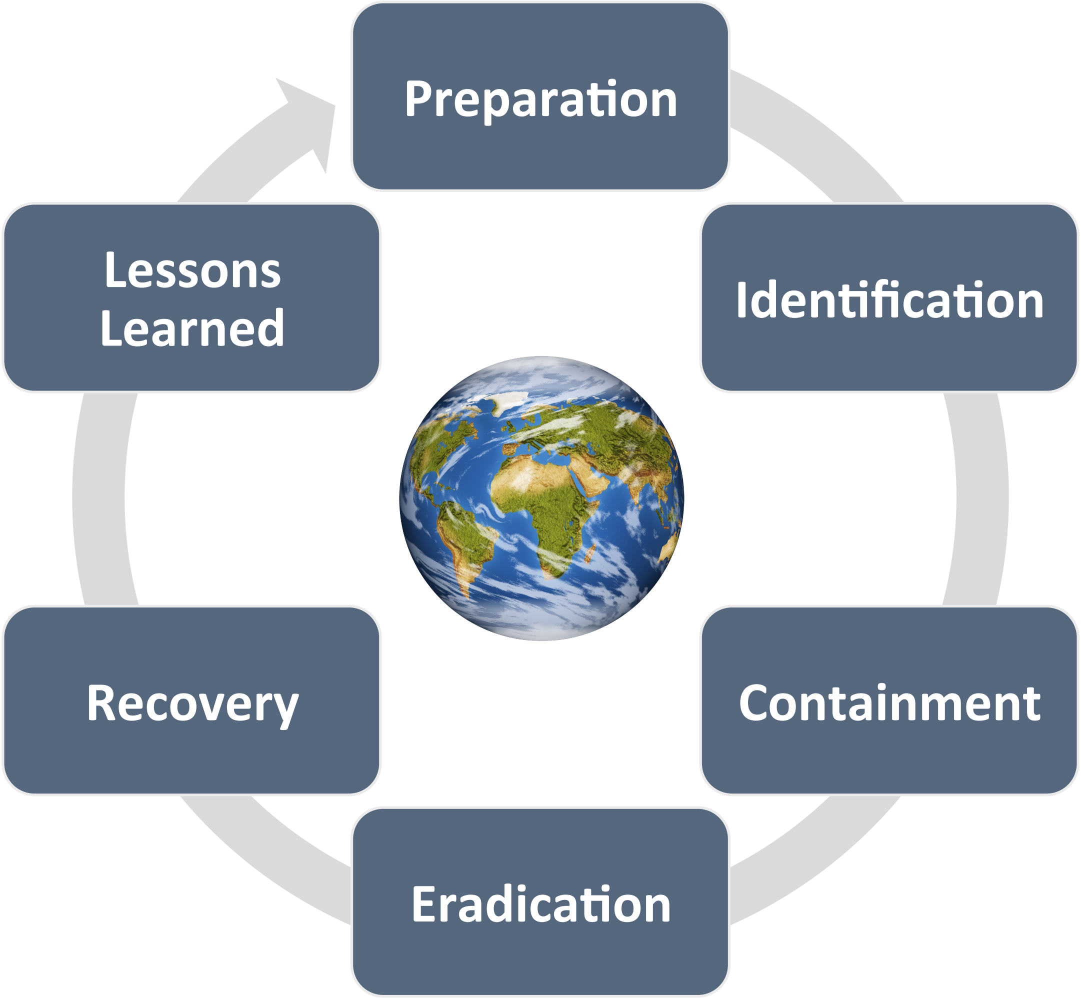
- Politics
- Strategy
- Trends in a sector, tender purchasing strategy
- Trade secrets, pricing discussions, competitor pricing information
- Gain a competitive edge
- Insider trading

According to Symantec, 70% APT victims profile

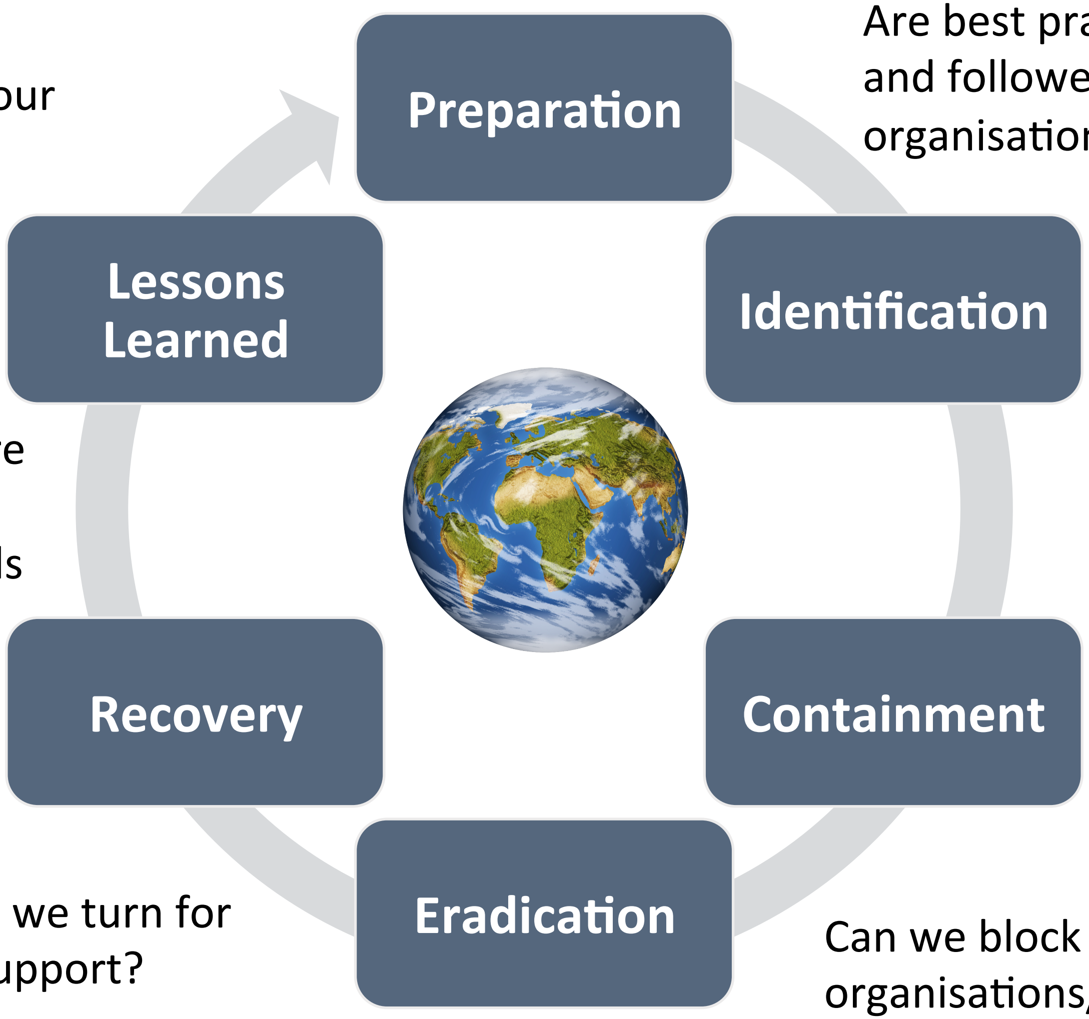
- Research, innovation, IT.
- "forward looking technologies" highly sellable

Besides.. customers may not know that our data is publicly available!

Incident response



Incident response



Preparation

Identification

Containment

Eradication

Recovery

Lessons Learned

Are best practices understood and followed at all participating organisations?

Are we able to contact external security contacts?

Do our logs show all connection activity?

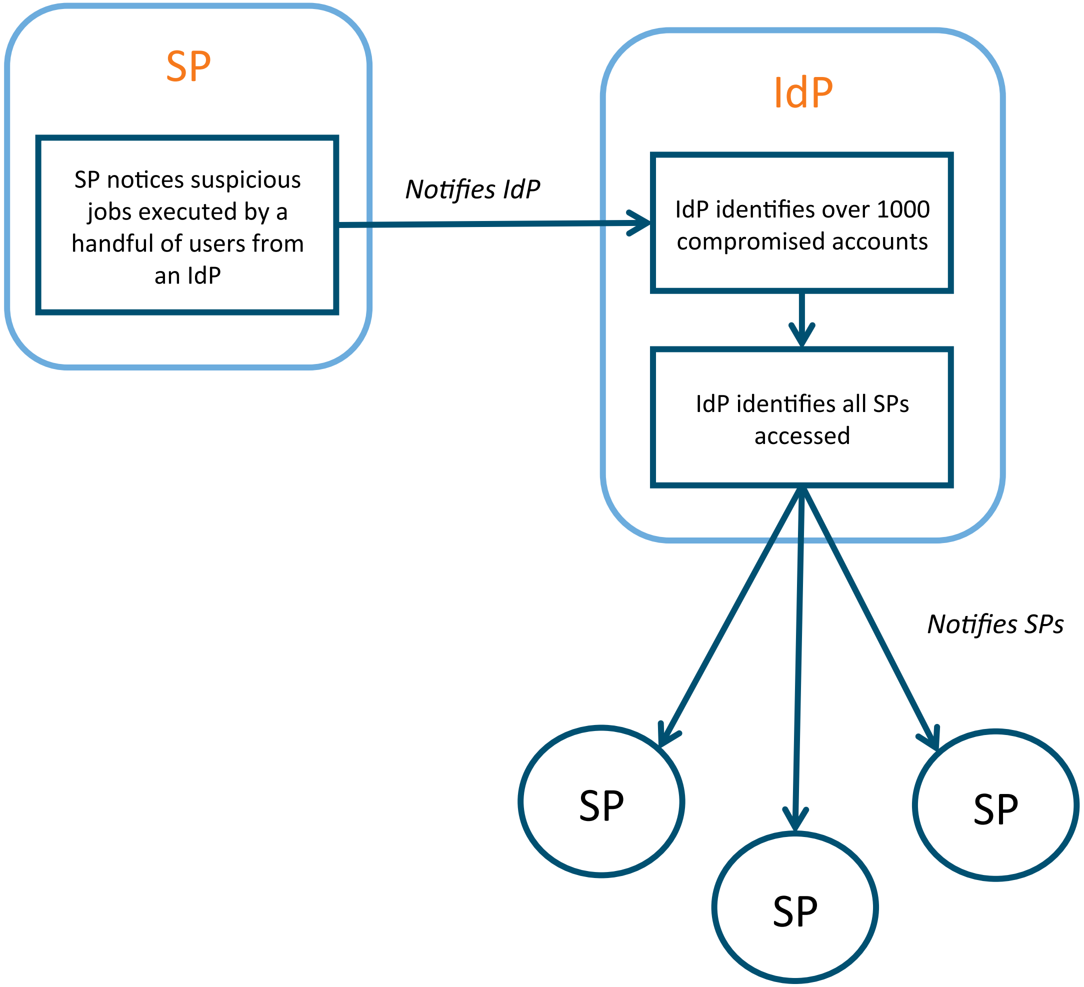
Can we block certain organisations/users

Where can we turn for help and support?

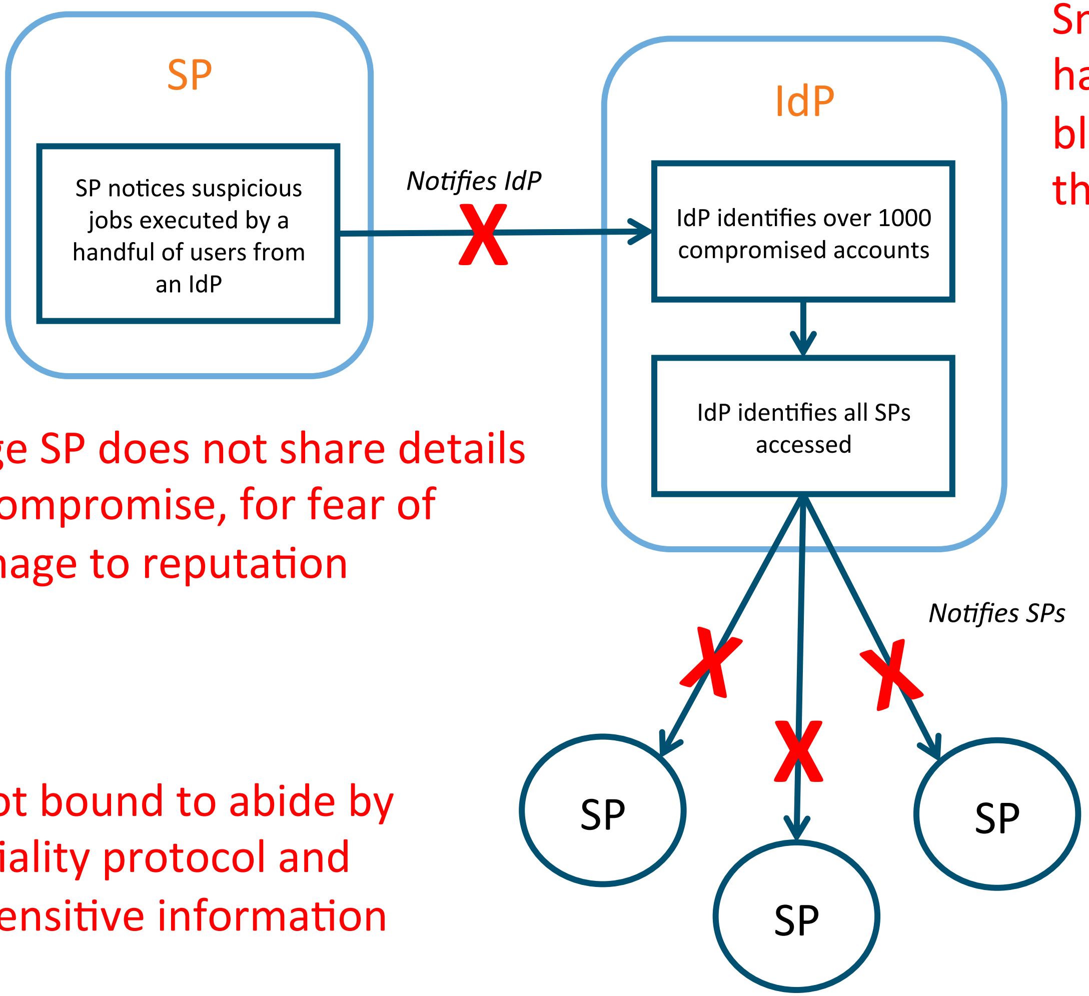
How can we share eradication and recovery methods

Can we pool our knowledge?

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
SP
SP
SP

But in reality…


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

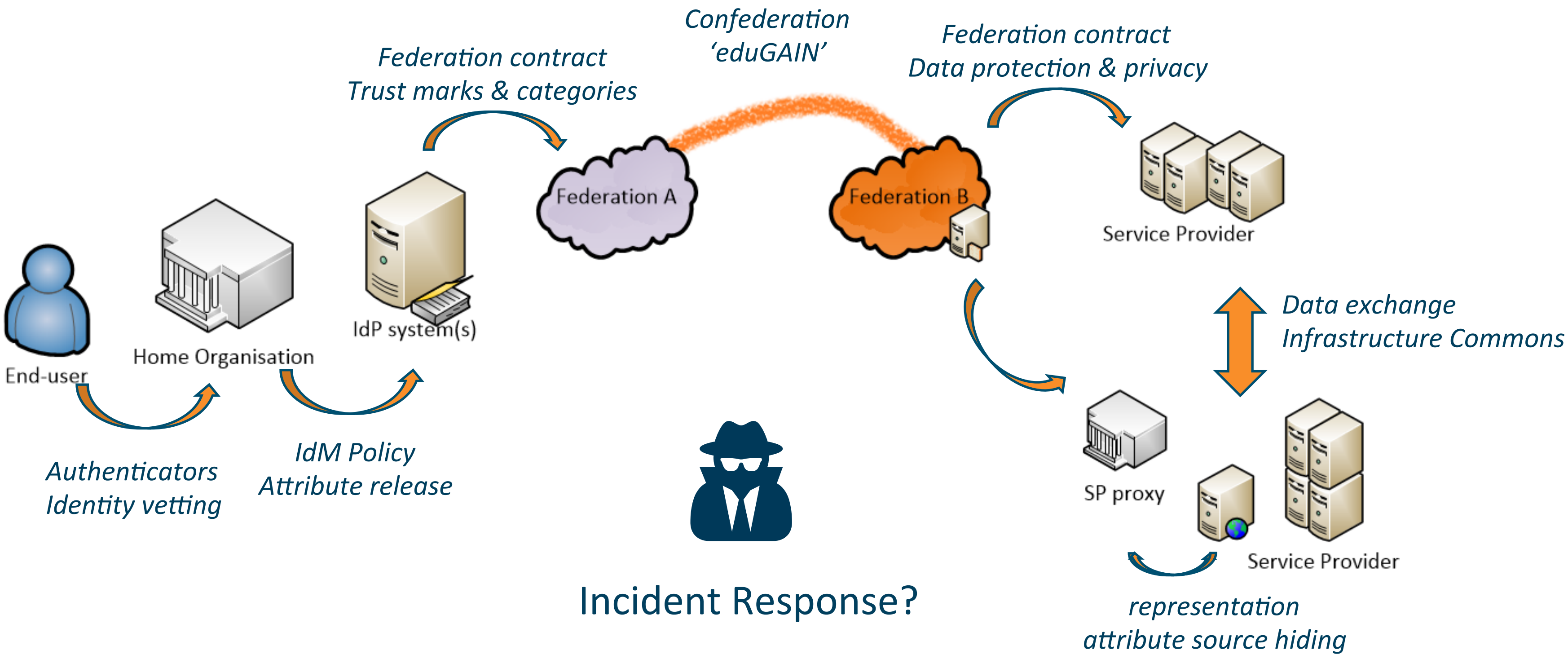
Small IdP may not have capability to block users, or trace their usage

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!

The chain of assurance



Authenticators
Identity vetting

IdM Policy
Attribute release

Federation contract
Trust marks & categories

Confederation
'eduGAIN'

Federation contract
Data protection & privacy

Data exchange
Infrastructure Commons

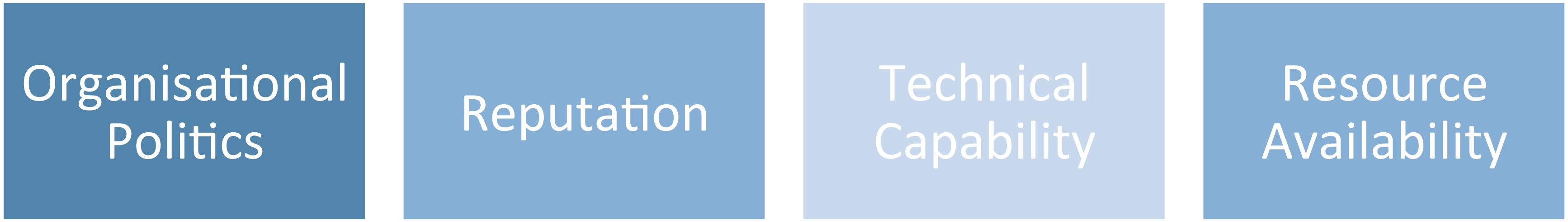
representation
attribute source hiding

Incident Response?

Credit to David Groep - Nikhef

Raising trust between organisations

- Despite shared policies in interfederation, the level of trust is often insufficient for effective collaboration during incident response



Organisational Politics

Reputation

Technical Capability

Resource Availability

- What we need is a…
  Security Incident Response Trust framework for Federated Identity

What is Sirtfi?

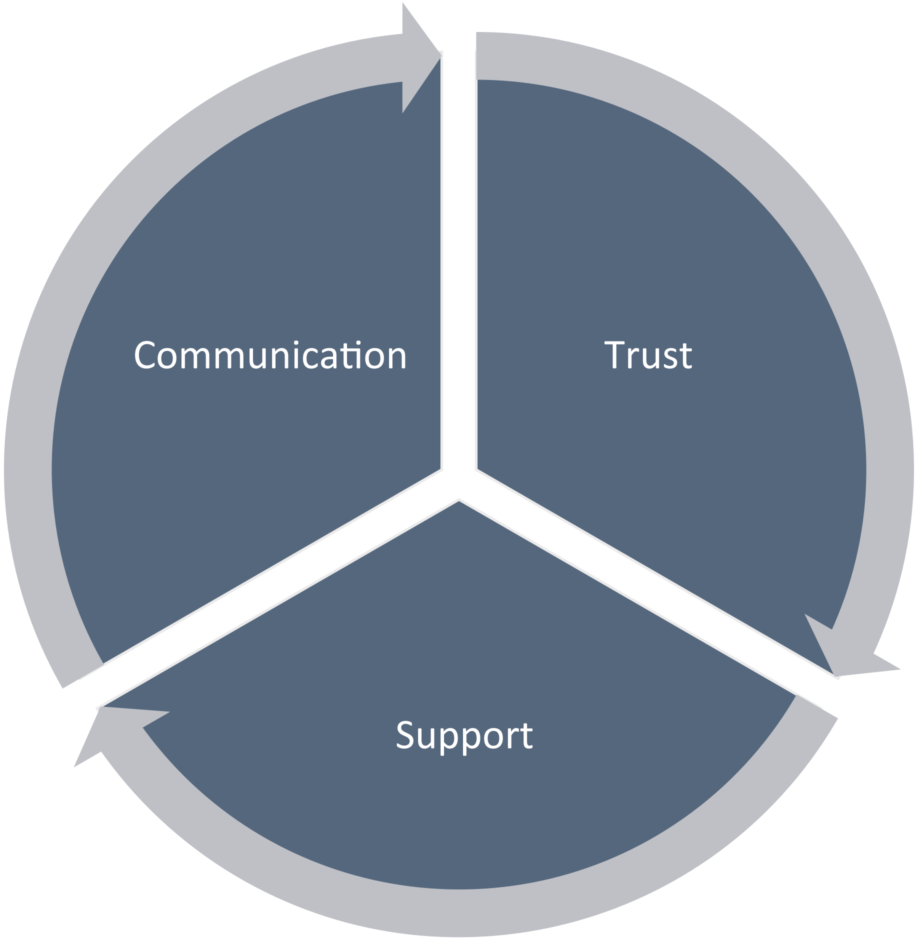
- A way to ensure that organisations within a federation are technically able and willing to participate in federated incident response

- A series of best practice statements in
  - Operational Security
  - Incident Response
  - Traceability
  - Participant Responsibilities

- If an organisation can say "I agree" to each and every statement, they are Sirtfi Compliant

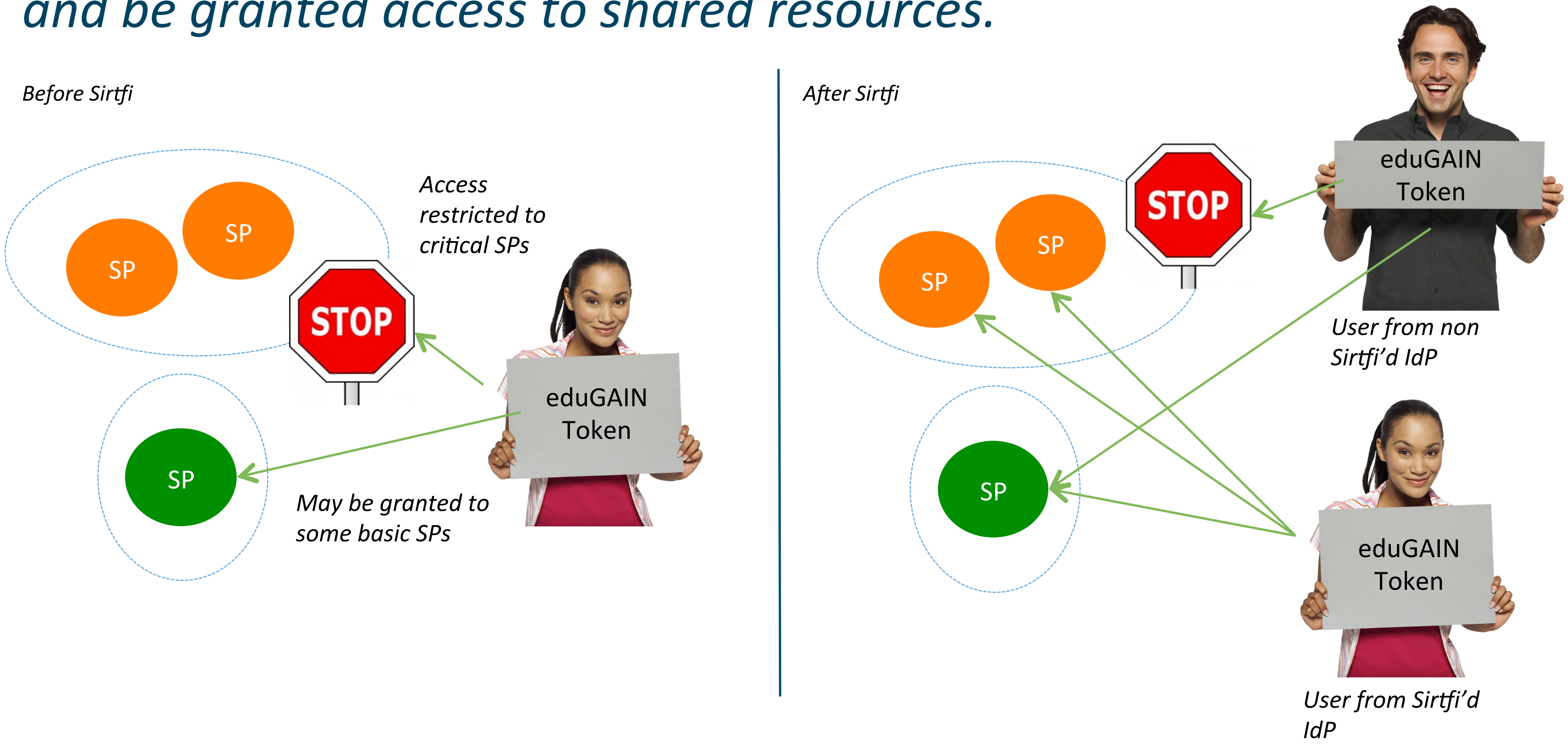
https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf

What will Sirtfi change?



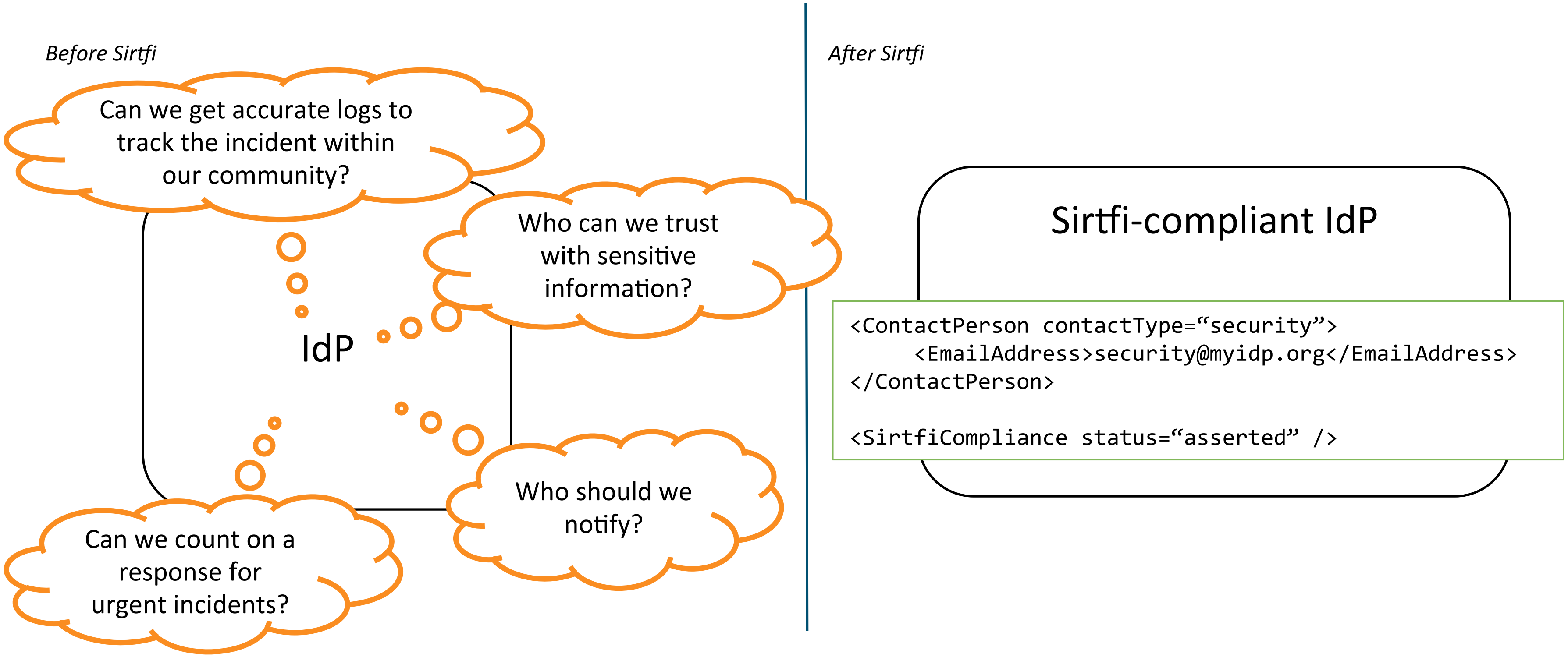
Trust

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.



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

IdP

Can we get accurate logs to track the incident within our community?

Who can we trust with sensitive information?

Can we count on a response for urgent incidents?

Who should we notify?

After Sirtfi

Sirtfi-compliant IdP

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

<SirtfiCompliance status="asserted" />
```

Communication

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…
```

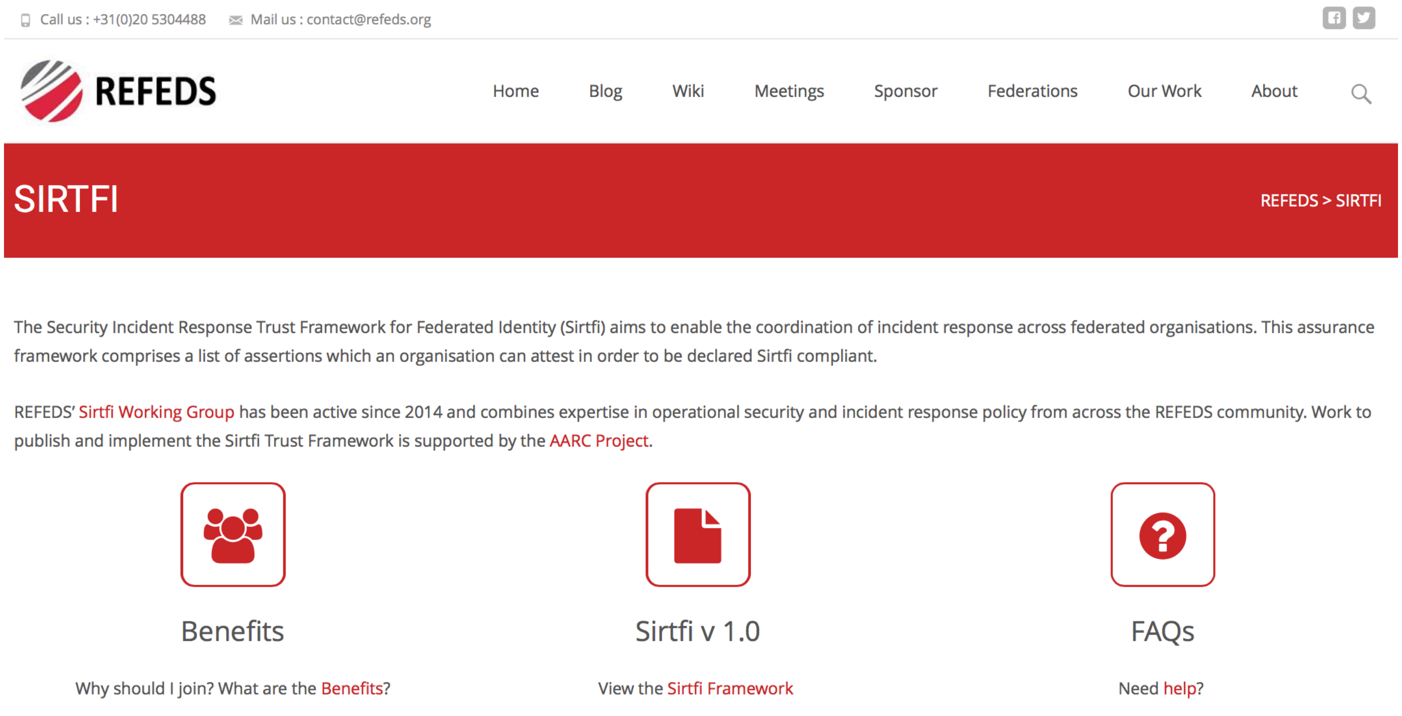
```
To: panic_stations@mysp.org
Cc: security@myidp.org
From: hero@myidp.org

**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.
```

Where to begin with Sirtfi?

- Training material in progress
- https://refeds.org/sirtfi



Call us : +31(0)20 5304488   Mail us : contact@refeds.org

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?

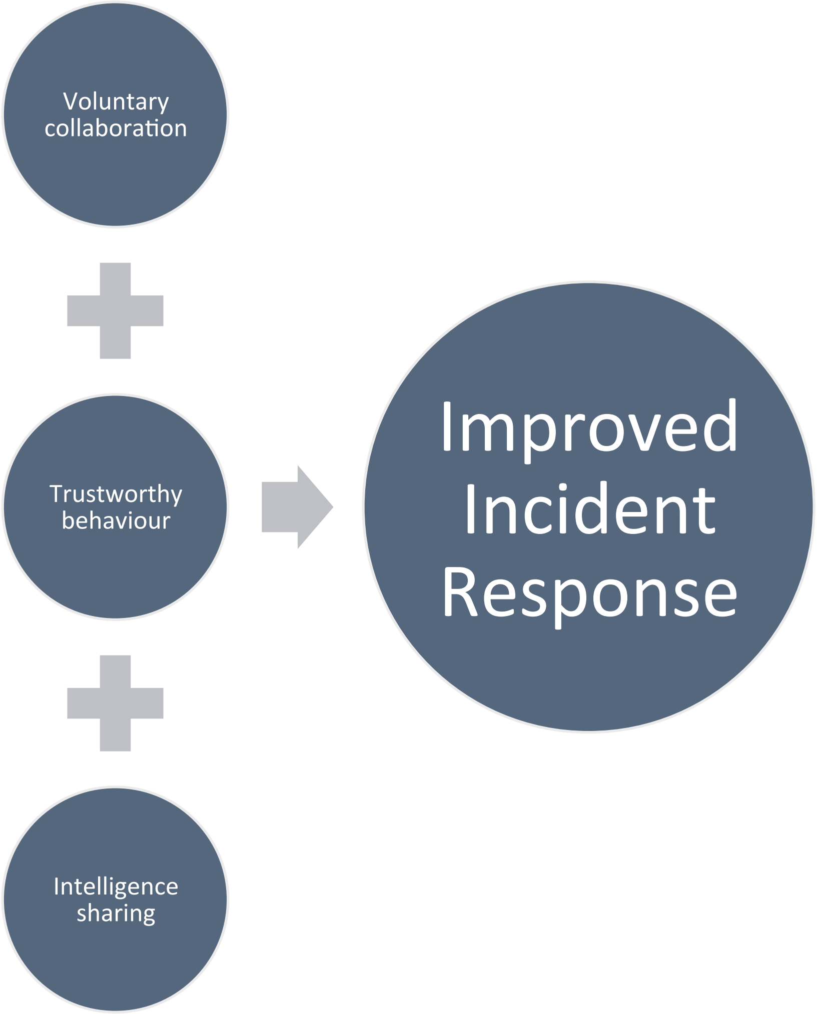
Building trust between individuals

- It is unrealistic to expect each organisation to employ experts in security response
  - Can leverage the expertise of security colleagues throughout the interfederation network
- Lack of trust between individuals is a block to information flow
- Individual relationships are able to traverse barriers
  - Political
  - Geographical
  - Cultural
- Go for a beer!

Trust groups

- Cyber-security threat intelligence trust groups exist, e.g. REN-ISAC in the US

- Being proactive in incident response collaboration boosts your personal credibility and opens doors to increasingly useful trust groups



Real World Example

We were given access to a botnet credential dump through trusted contacts…

CERN ACCOUNT

WLCG User

What kind of incident is this??

Account with US University

Faculty rights at US University

Further accounts in research organisations

Accessed Federated Services!

Conclusion

- The federated landscape
- Common vectors of attack
- Incident response
- Building trust between organisations
- Building trust between individuals

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).