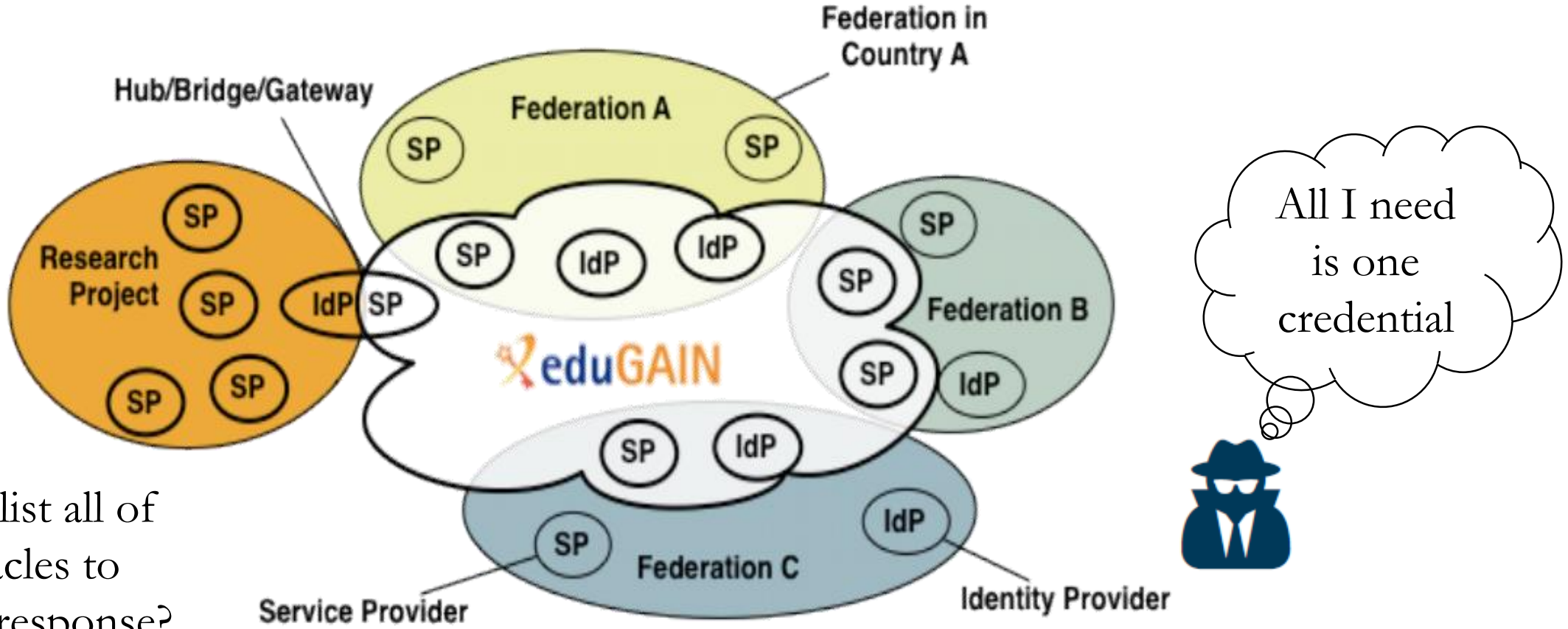
Security Incident Response

10th FIM4R Workshop
February 2017

Tom Barton
University of Chicago & Internet2

The problem of security incident response in a federated system



Can you list all of the obstacles to incident response?

SIRTFI
Security Incident Response Trust Framework for Federated Identity

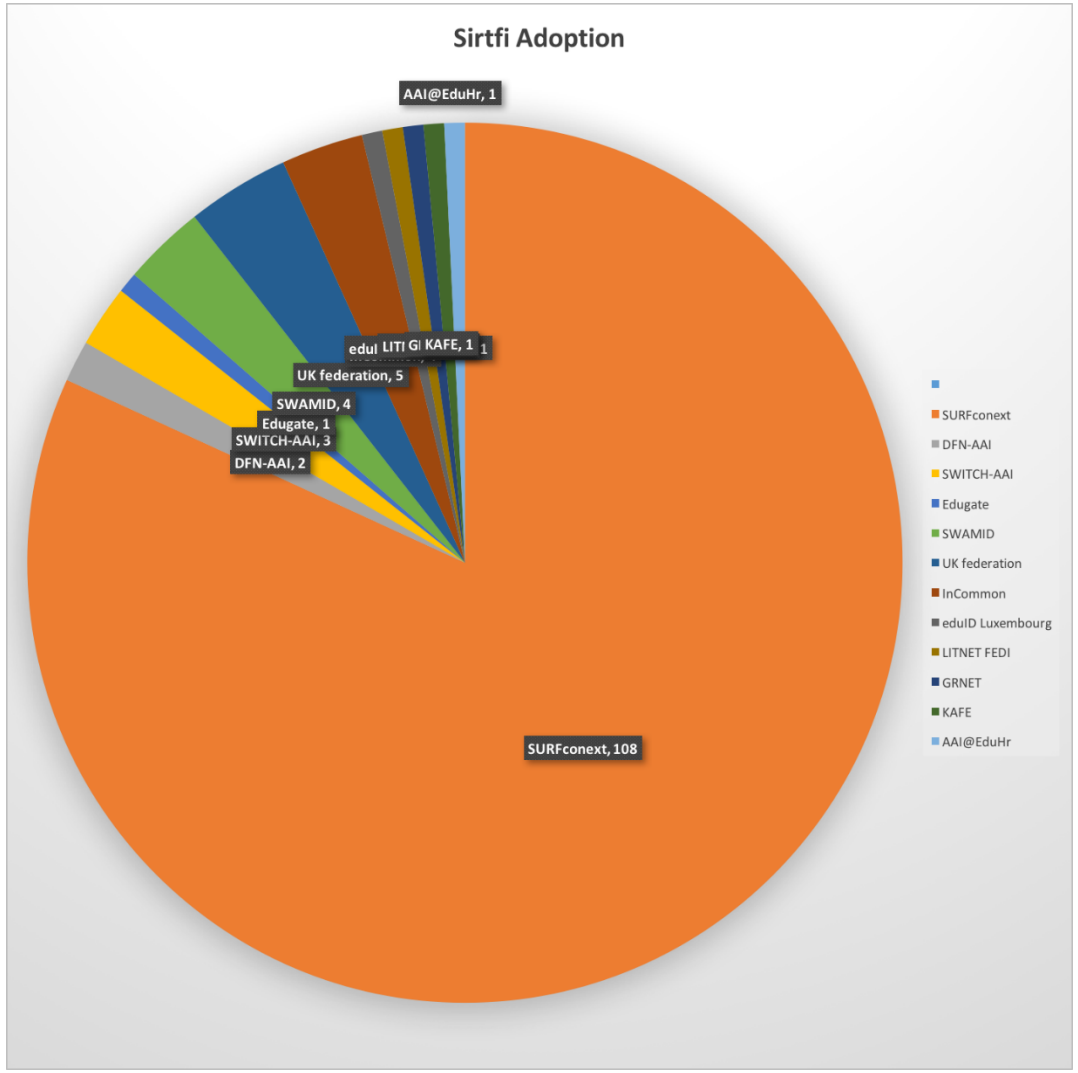
Picture/ideas courtesy of Ann Harding, Hannah Short

- **S**ecurity **I**ncident **R**esponse **T**rust Framework for **F**ederated **I**dentity
- Working Group established to address the problem
  - REFEDS, AARC, GÉANT supported
  - Many perspectives represented: federation, security, research CI, campus, Europe, North America
- ~ 2 years of work completed (and longer: FIM4R and SCI foundations)
  - Entity and Participant-level standards, educational materials, initial adoption
- ~ 2 more years of work remain
  - Inter/Federation standards and services, tooling, much more outreach & adoption

Work plan - accomplished

Sirtfi v1.0	Baseline requirements for Entity/Participant security operations and coordination
Security contact metadata schema	Where to initiate response
IANA assurance entity attribute registered	To mark Entities that conform to Sirtfi
Sirtfi Identity Assurance Certification Description	Normative guidance to federation operators in maintaining the above
Educational materials for the above	https://wiki.refeds.org/display/SIRTFI/SIRTFI+Home

Initial adoption



- 29 R&E Federations support or plan to support Sirtfi
  - 4 no plan, 33 unknown
- 2 R&E Feds have comprehensive support
- 135 Sirtfi-tagged entities, mostly IdPs
- 639 entities with security contact info

SIRTFI
Security Incident Response Trust Framework for Federated Identity

Work plan – ahead draft 1/2

Survey/outreach to federations	Learn status and how to help them adopt	GN4
Tooling	• Response support "platform" • Lookup/notify Sirtfi-tagged SPs that have been accessed by a given IdP credential	GN4 WG
Federated Security Incident Response Procedures (derivative of AARC DNA3.2)	Framework in which Participants, Federation Operators, and the eduGain Operator coordinate response to a security incident	WG AARC
Security Incident Response Plan for a Federation Operator	Template/starting point to help R&E Federations establish security procedures	WG
Incorporate research CIs into above (Snctfi)	Security incident response procedures and tooling should suitably integrate with research CIs	FIM4R WG

SIRTFI
Security Incident Response Trust Framework for Federated Identity

Work plan – ahead draft 2/2

More tooling	• Online self-assessment for Participants • Online courseware	GN4 WG AARC
Sirtfi v2	Revise v1 to incorporate obligation to notify of access to a Sirtfi SP by a compromised credential	WG
Further educational materials	Supporting new standards, tools, etc.	WG
Get the word out; gain input and participation	• Which groups and organizations should we loop in? • What events should we aim to participate in?	WG AARC FIM4R ???

SIRTFI
Security Incident Response Trust Framework for Federated Identity