AARC Authentication and Authorisation for Research and Collaboration

Testing Incident Response Channels and Communications End Points – and their capabilities

whilst not overloading the target audience

David Groep

AARC Policy and Best Practice Activity Coordinator

Nikhef

Nikhef

WISE and SIG-ISM meeting Kaunas

April 2019

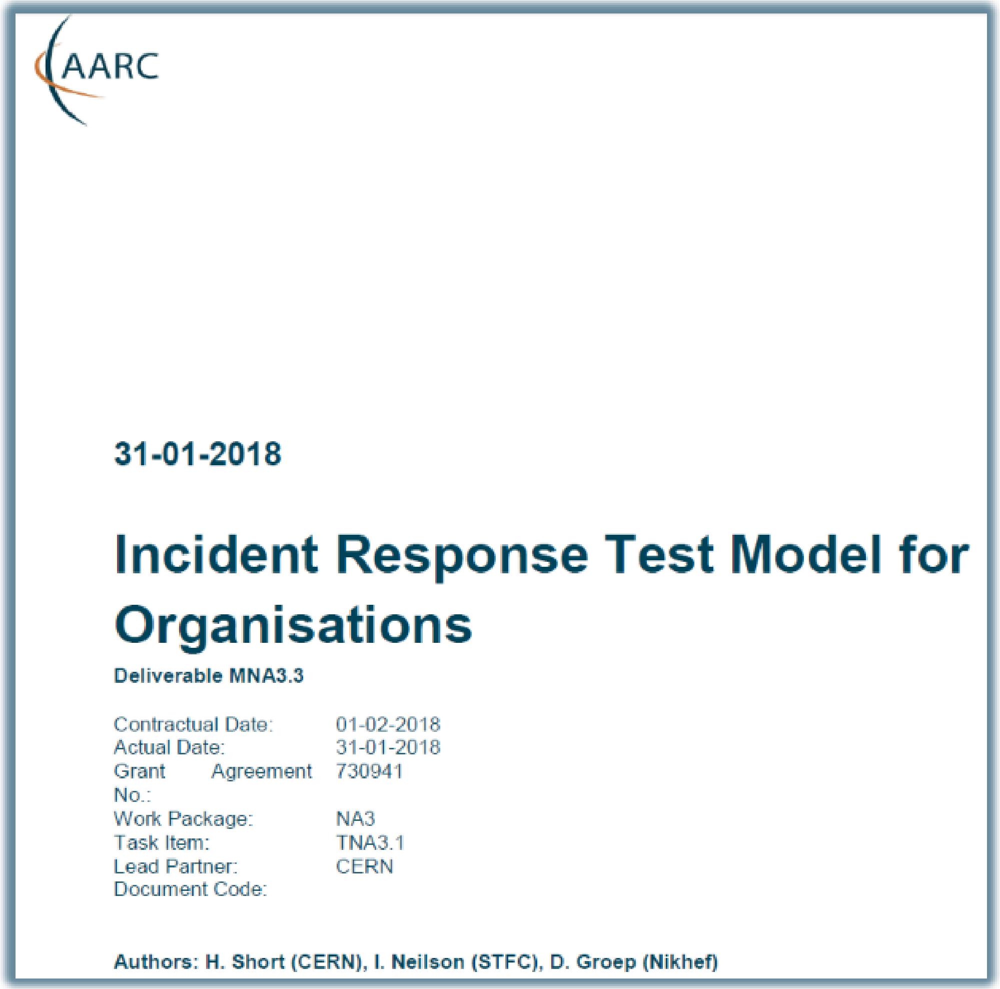
Distributed Incident Response and Readiness Challenges

Sirtfi - version 1 - is gaining traction

- provides - self-asserted - security contacts
- point-to-point communications
- shows interaction not usually visible at the ‘global’ level

now we need to now go ‘beyond *Sirtfi*’

- incidents are not usually bi-lateral
- may spread through federated identity systems
- and outside to relying parties or entire Infrastructure



AARC

31-01-2018

Incident Response Test Model for Organisations

Deliverable MNA3.3

Contractual Date:	01-02-2018
Actual Date:	31-01-2018
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	TNA3.1
Lead Partner:	CERN
Document Code:	

Authors: H. Short (CERN), I. Neilson (STFC), D. Groep (Nikhef)

Responding to incidents – sharing relevant information

- Sirtfi take-up at proper organizational level

Beyond basic Sirtfi

- federation-level engagement in process
- *Sirtfi+* registry broadens global base
- engagement in trust groups valuable for federated collective response

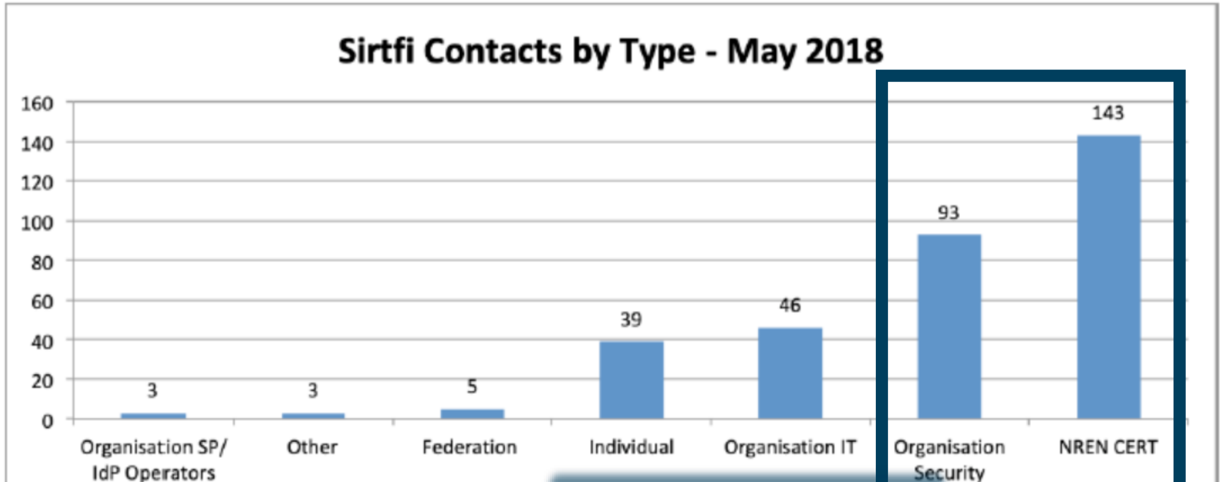
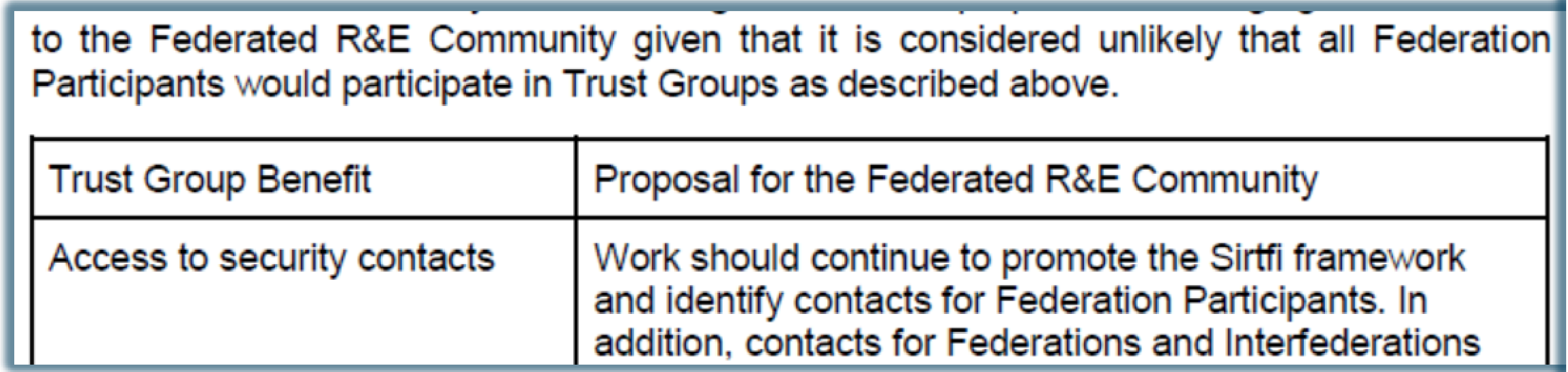
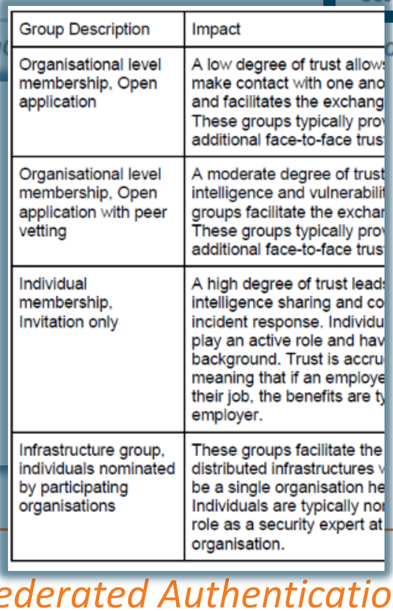


Figure 2: Sirtfi contacts as listed in the edu d by contact type.


to the Federated R&E Community given that it is considered unlikely that all Federation Participants would participate in Trust Groups as described above.

Trust Group Benefit	Proposal for the Federated R&E Community
Access to security contacts	Work should continue to promote the Sirtfi framework and identify contacts for Federation Participants. In addition, contacts for Federations and Interfederations



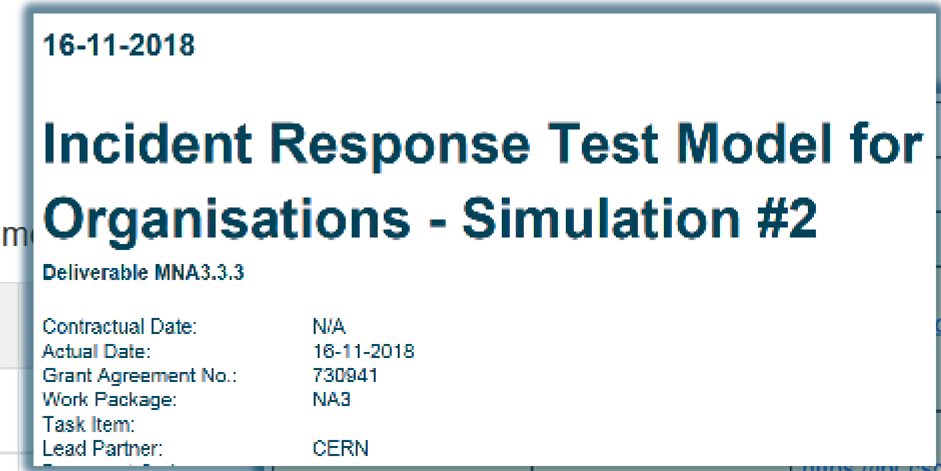
Group Description	Impact
Organisational level membership, Open application	A low degree of trust allows make contact with one ano and facilitates the exchang These groups typically prov additional face-to-face trus
Organisational level membership, Open application with peer vetting	A moderate degree of trust intelligence and vulnerabilit groups facilitate the exchan These groups typically prov additional face-to-face trus
Individual membership, Invitation only	A high degree of trust leads intelligence sharing and co incident response. Individu play an active role and hav background. Trust is accru meaning that if an employe their job, the benefits are t employer.
Infrastructure group, individuals nominated by participating organisations	These groups facilitate the distributed infrastructures v be a single organisation he Individuals are typically nor role as a security expert at organisation.

from DNA3.2 *Report on Security Incident Response and Cybersecurity in Federated Authentication Scenarios*

… the rest we test …

In AARC2 we will further the work undertaken in AARC and provide a fram

Month	What	
9	Incident Response Test Model for Organizations **MNA3.3**	
10	Incident Simulation #1 Report	https://aarc-pr
19	Incident Simulation #2 Report	https://aarc-p
?	Guideline on Incident Response for Federation Participants	Draft at https:
22	Report on Security Incident Response **DNA3.2**	Draft at https:

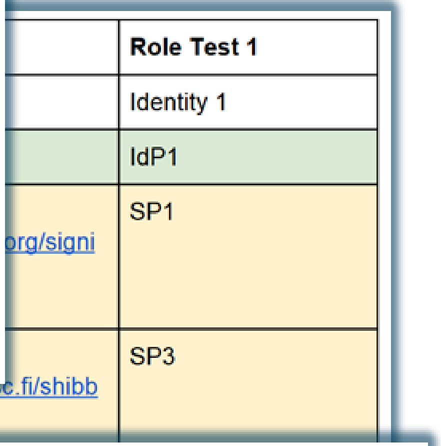


16-11-2018

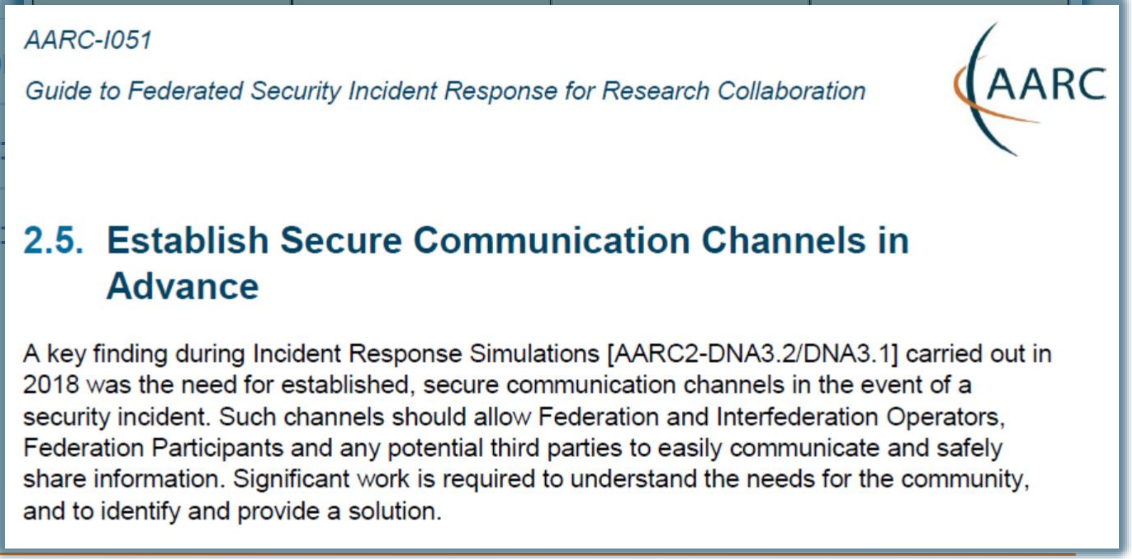
Incident Response Test Model for Organisations - Simulation #2

Deliverable MNA3.3.3

Contractual Date:	N/A
Actual Date:	16-11-2018
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	
Lead Partner:	CERN



	Role Test 1
	Identity 1
	IdP1
org/signi	SP1
https://ibr.csc.fi/shibb oleth	SP3



AARC-I051

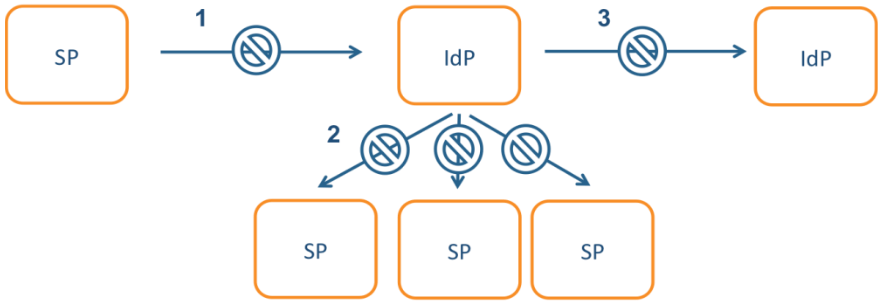
Guide to Federated Security Incident Response for Research Collaboration

2.5. Establish Secure Communication Channels in Advance

A key finding during Incident Response Simulations [AARC2-DNA3.2/DNA3.1] carried out in 2018 was the need for established, secure communication channels in the event of a security incident. Such channels should allow Federation and Interfederation Operators, Federation Participants and any potential third parties to easily communicate and safely share information. Significant work is required to understand the needs for the community, and to identify and provide a solution.

https://wiki.geant.org/display/AARC/AARC2+NA3+Task+1+-++Overview
https://aarc-project.eu/guidelines/aarc-i051/

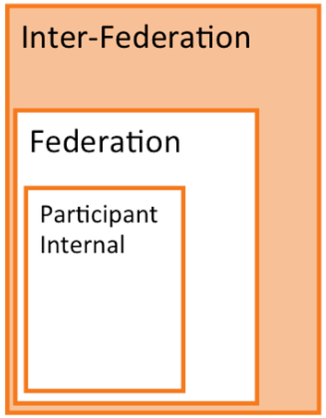
Incident response process evolution in federations



Incident Response Communication, communication blocks

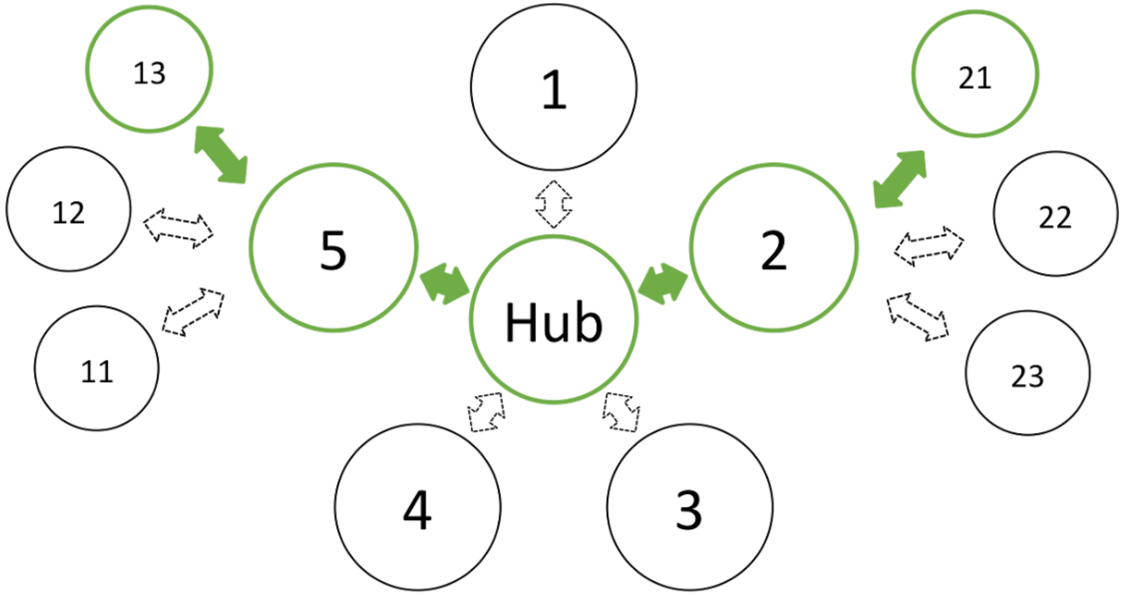
Challenges

- IdP appears ‘outside’ the service’s security mandate
- Lack of contact, or lack of trust, in IdP, which is an ‘unknown party’
- IdP fails to inform other affected SPs, for fear of leaking data or reputation
- No established channels of communication



Proposed solutions

- Stronger role for federation operators, as they are known to both SPs and IdPs
- Add hub capability centrally (@ eduGAIN)



Inter-Federation Incident Response Communication

graphics: Hannah Short, AARC ‘DNA3.1’ incident response models

Who runs the test?

The first tests with these participants were run ‘by AARC’

Logical candidates that could all run the test

… and have an interest in knowing the result to establish trust

- eduGAIN
- GEANT.org
- but also any EOSC-HUB and e-Infrastructure CSIRT teams
- the IGTF (as it leverages federated id)
- each of the e-Infrastructures XSEDE, EGI, EUDAT, PRACE, OSG, HPCI, …
- every research infra with an interest: WLCG, LSAAI, BBMRI, ELIXIR, …

And any institution (or person) with access to https://mds.edugain.org/ can run them, of course

so in a short while, all the email in the world will be on Sirtfi Incident Response tests??

Frequency of challenges and tests - examples

Trusted Introducer and TF-CSIRT

- 2-3 Reaction Tests per year
- supported by web click infrastructure, but requires (team) authentication

SURFcert challenges

- annual response challenges, just reply to email to a (traceable) ticket

IGTF RAT Communications Challenges

- every 1-2 years
- in parallel with continuous operational monitoring

yet we already listed 14 entities that have a real interest in running tests, 5000+ entities can claim the same

Challenge elements – what is valued or expected might differ …

- timeliness
- investigative capability
- confidentiality
- ability to take action
- ….

but a single test can answer the questions of many

- if the challenge measures responsiveness and the data are available, each infrastructure can set its *own level* of expectancy

but other elements require different probes (and may be complex or intensive to conduct)

- responsiveness vs. ability to take action or forensics/traceability capacity

How to coordinate – discussion items!

Designate a lead ‘management’ organization for each element?

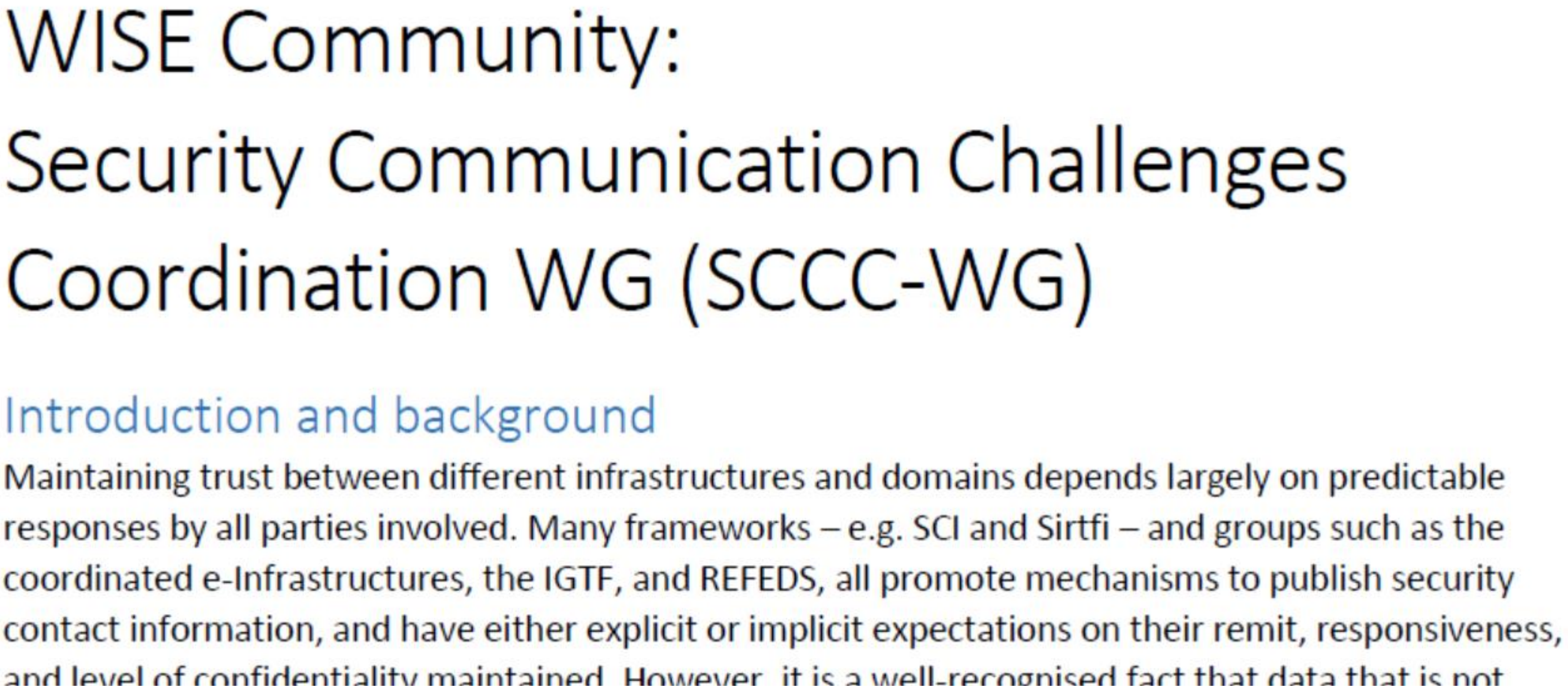
so that each ‘target’ does not get hit by many competing and concurrent challenges?

- e.g. eduGAIN to run communications challenges against Sirtfi email addresses
- the e-Infrastructures to test responsiveness of SPs and RPs
  with each RP/SP/Site having a primary e-Infra as its home?
  or can we jointly (EOSC-HUB) run these challenges per continent?
- coordination must be global

Communications challenges also build ‘confidence’ and trust – an important social aspect

- unless you run the test yourself, or get full insight in the results of a challenge,
  you may not be growing more trust in the entities tested
- so to get that ‘warm and fuzzy feeling of trust’,
  results (responsiveness measurement data) should be shared
  but that sharing needs to be confidential as well – limit to WISE SCI checked infrastructures?

Towards SCCC WG …



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, and level of confidentiality maintained. However, it is a well-recognised fact that data that is not

Proposal for the SCCC Working Group

Coordination of ‘CCs recipient groups’ among participating infrastructures

- ensure targets are not overloaded by coinciding or overlapping challenges, for example by designating lead agency

Transitivity of trust in CC results between infrastructures

- for example by specifying the level of disclosure detail for CCs between trusted infrastructures, by using an SCI evaluation framework approach to it, or by coordination of testing and success criteria.
- how can requests for CCs between infrastructures be handled, e.g. in response to changing needs or a changed risk assessments; or as remediation after an incident in which communications did not meet expectation.

Definition of CC models and classification

- ‘depth’ of the CC testing is a balance between the level of trust gained (more profound testing and good results gives more trust) and expediency (asking the recipient to respond to a mail or click a link consumes less resources than requesting forensic investigation of a simulated incident of deliberately unknown nature).

Frequency of CCs

- simple communications challenges are often performed one or several times per year (e.g. for TF-CSIRT, by SURFcert for the SURFconext federation, EGI Operations on their sites).
- complex challenges are less frequent (e.g. ‘black-box traceability’ trials in EGI take place once every 1-2 years).
- following a CC model classification, propose an appropriate frequency for each class.

Open Questions

- Members – interested parties, infrastructures, and their peers
- Standing coordination function through WISE

Thank you

Any Questions?

davidg@nikhef.nl

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. 730941 (AARC2).