AARC Authentication and Authorisation for Research and Collaboration

Get in touch – and be sure to get an answer?

Security Coordination Communications Challenges – all in it together

David Groep

AARC Community, policy and best practice area

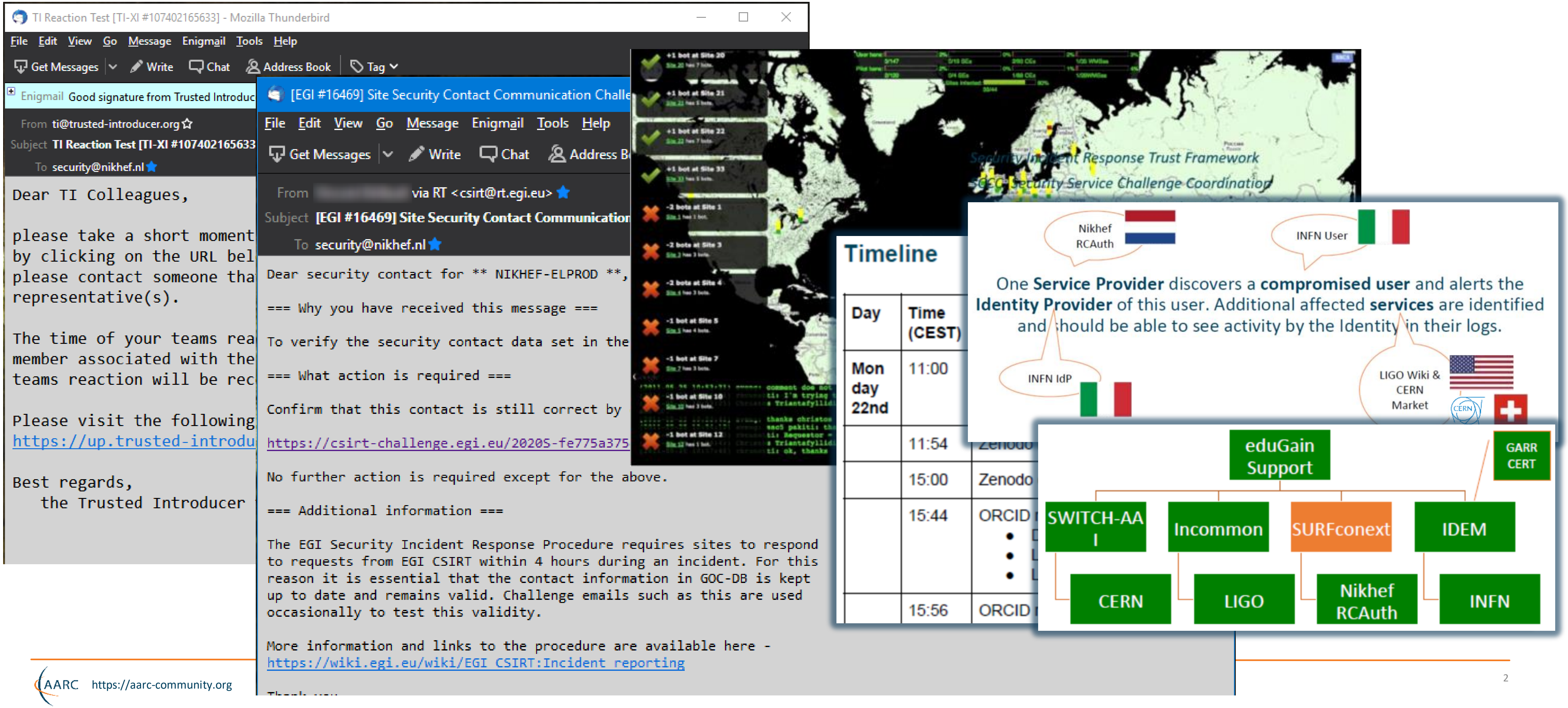
Nikhef PDP programme

Nikhef

WISE Community meeting

October 2020

Many communities test, test, and test again



TI Reaction Test [TI-XI #107402165633] - Mozilla Thunderbird

Enigmail Good signature from Trusted Introduc

From ti@trusted-introducer.org

Subject TI Reaction Test [TI-XI #107402165633

To security@nikhef.nl

```
Dear TI Colleagues,

please take a short moment
by clicking on the URL bel
please contact someone tha
representative(s).

The time of your teams rea
member associated with the
teams reaction will be rec

Please visit the following
https://up.trusted-introdu

Best regards,
   the Trusted Introducer
```

[EGI #16469] Site Security Contact Communication Challe

From [redacted] via RT <csirt@rt.egi.eu>

Subject [EGI #16469] Site Security Contact Communication

To security@nikhef.nl

```
Dear security contact for ** NIKHEF-ELPROD **,

=== Why you have received this message ===

To verify the security contact data set in the

=== What action is required ===

Confirm that this contact is still correct by

https://csirt-challenge.egi.eu/2020S-fe775a375

No further action is required except for the above.

=== Additional information ===

The EGI Security Incident Response Procedure requires sites to respond
to requests from EGI CSIRT within 4 hours during an incident. For this
reason it is essential that the contact information in GOC-DB is kept
up to date and remains valid. Challenge emails such as this are used
occasionally to test this validity.

More information and links to the procedure are available here -
https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting

Thank you
```

Security Incident Response Trust Framework

SCC Security Service Challenge Coordination

Timeline

Day	Time (CEST)	
Mon day 22nd	11:00	
	11:54	Zenodo
	15:00	Zenodo
	15:44	ORCID r • D • L • L
	15:56	ORCID r

One **Service Provider** discovers a **compromised user** and alerts the **Identity Provider** of this user. Additional affected **services** are identified and should be able to see activity by the Identity in their logs.

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

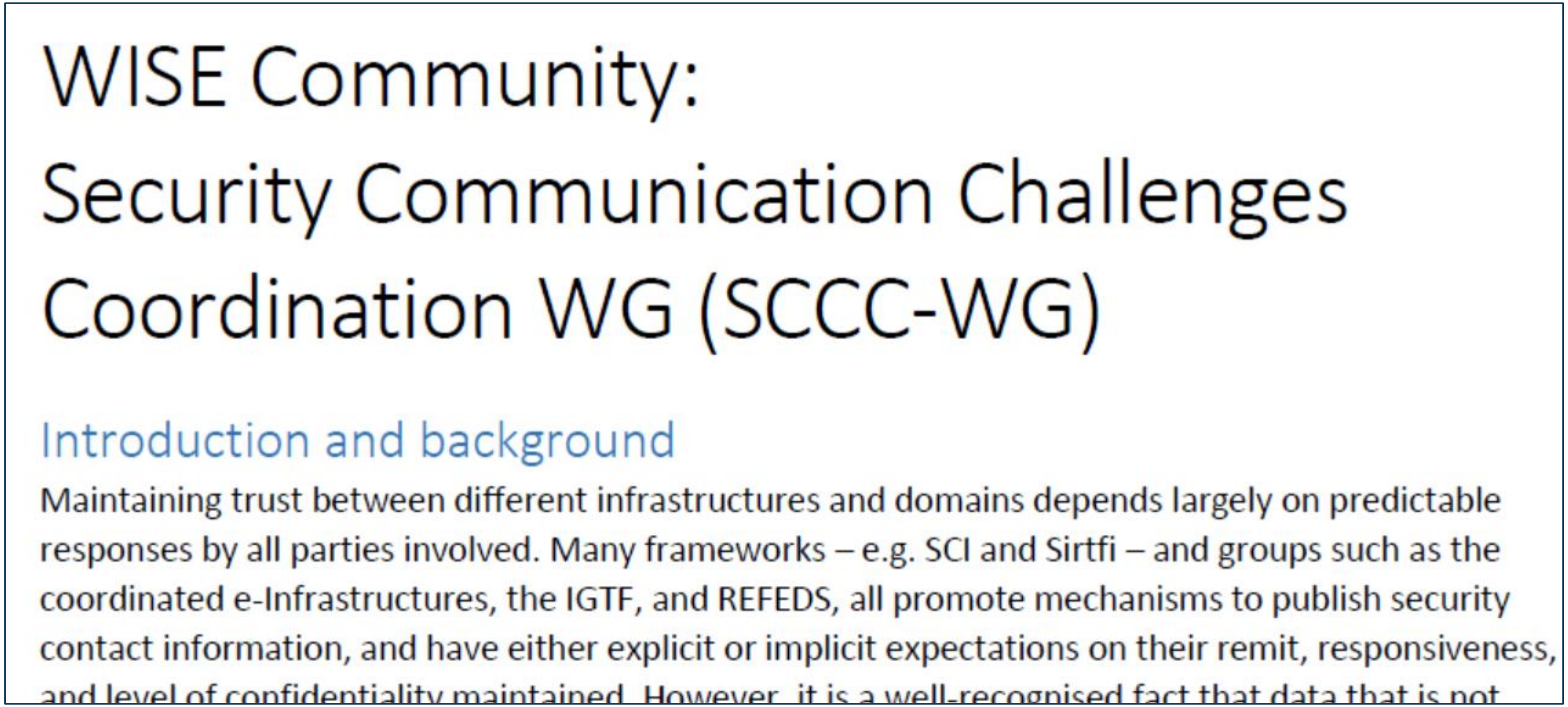
SURFcert challenges

- 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

Continued engagement and coordination: WISE SCCC JOINT 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

WISE

SIG-ISM

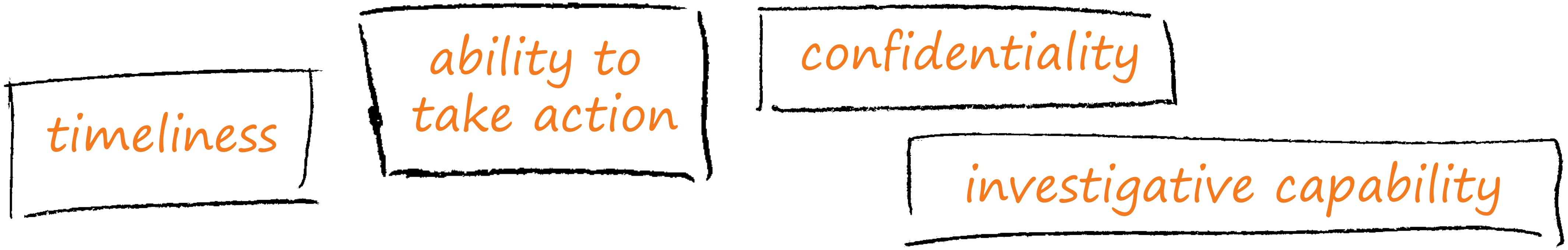
REFEDS

IGTF

https://wiki.geant.org/display/WISE/SCCC-JWG

Challenge elements – what is valued or expected might differ …

A single test and challenge can answer one **or more** of these questions



timeliness

ability to take action

confidentiality

investigative capability

- when data available: infrastructure can set its *own level* of expectancy and gives *deep trust*
- assessment supported with community controls (suspension) gives a *baseline compliance*

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

- different tests bring complementary results: responsiveness vs. ability act , or do forensics
- unless you run the test yourself, you may not be growing more trust in the entities tested
- for a ‘warm and fuzzy feeling of trust’, share results: but this is sociologically still challenging …

Addressing a ‘new’ community – eduGAIN entities

‘community is not new, but doing multi-federation security communications therein is’

- Still only 939 (in 36 federations) assert *Sirtfi* … out of 7149 entities (13%)

Quite some open questions

- Are the other entities unaware, or actually not interested?
- In an ongoing incident, can we reach them nevertheless? Even just to establish a channel?
- The contact we *do* have, do they react? Do *Sirtfi* contacts react faster?
- Or maybe is formally asking for a ‘security’ contact setting off a chain of bureaucracy?

For a first challenge, start with a ‘gameifiable’ responsiveness challenge

and leave log analysis, forensics, and the more complex elements of Sirtfi out of scope

Gradual approach – introducing comms challenges in eduGAIN

A community with ‘a wide diversity in terms of comms challenge acquaintance’

- Not even all federation have a designated security contact
  but maybe because a formal assignment of such a role is considered daunting responsibility?

Target:

- **end-entities** – initially in some friendly federations that will opt-in all their entities
- **security contacts** if available, otherwise try **technical contact** (and ask for security contact)

- run by the federation (using the software), but also offered ‘as a service’ - supported through Trust and Identity activity (eduGAIN Security and Enabling Communities jointly) – and branded with the federation email address and names.
  Sven & Daniel can re-use the existing EGI software tooling for that, on a VM provided with an .edugain.org domain

https://codimd.web.cern.ch/Fx1LO0O3TrOq_YxkzSMpxw

Subsidiary aim: make security contacts less ‘scary’

The most basic response is to (sorry!) click on a harmless link: making it a challenge to respond ‘as fast as possible’ – a bit like a competition

Ask also a very simple ‘question’ to raise awareness,

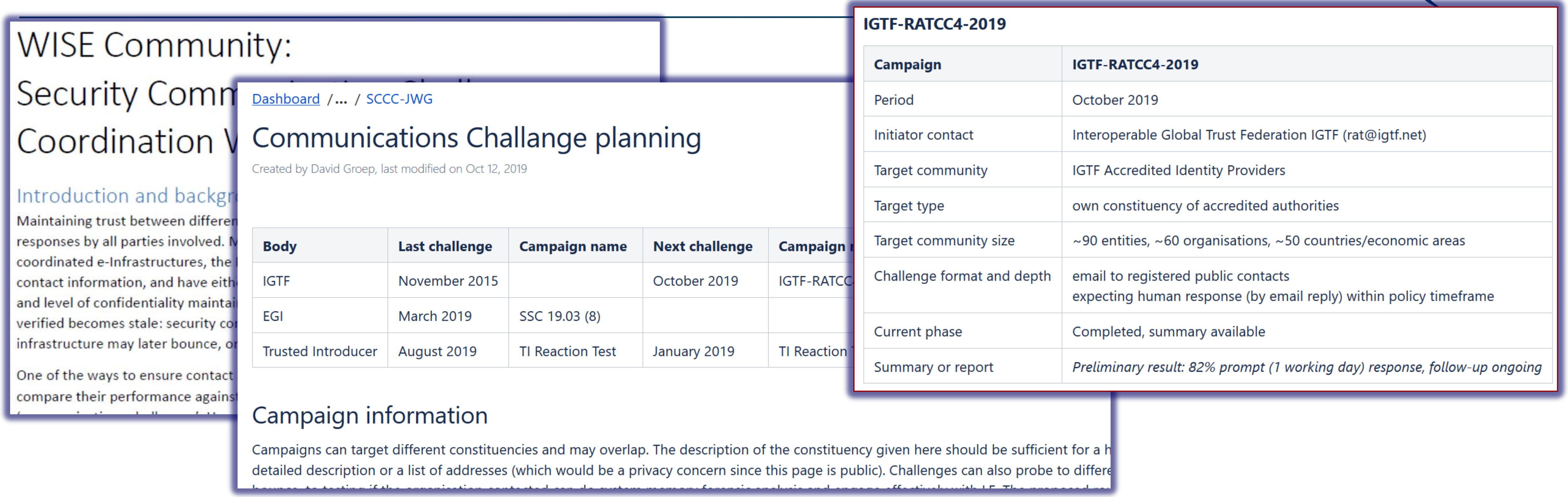
> ‘for security contacts, do you want to be (proactively) informed if we have security information relevant to your organisation?’

***esp.* if the contact is the technical rep, i.e. there is no *Sirtfi* contact**

> ‘you got this message because there is no designated security contact for your organisation. Would you want to receive security information, or who (if not you) should be your security contact?
> Are you aware of Sirtfi?’

And we can add some ads for Sirtfi, although having *any* kind of contact is better than none …

WISE SCCC-WG – participate!



WISE Community:
Security Comm
Coordination W

Introduction and backgr

Maintaining trust between differen
responses by all parties involved. M
coordinated e-Infrastructures, the I
contact information, and have eith
and level of confidentiality maintai
verified becomes stale: security co
infrastructure may later bounce, or

One of the ways to ensure contact
compare their performance against

Dashboard / ... / SCCC-JWG

Communications Challange planning

Created by David Groep, last modified on Oct 12, 2019

Body	Last challenge	Campaign name	Next challenge	Campaign n
IGTF	November 2015		October 2019	IGTF-RATCC
EGI	March 2019	SSC 19.03 (8)		
Trusted Introducer	August 2019	TI Reaction Test	January 2019	TI Reaction

Campaign information

Campaigns can target different constituencies and may overlap. The description of the constituency given here should be sufficient for a h
detailed description or a list of addresses (which would be a privacy concern since this page is public). Challenges can also probe to differe

IGTF-RATCC4-2019

Campaign	IGTF-RATCC4-2019
Period	October 2019
Initiator contact	Interoperable Global Trust Federation IGTF (rat@igtf.net)
Target community	IGTF Accredited Identity Providers
Target type	own constituency of accredited authorities
Target community size	~90 entities, ~60 organisations, ~50 countries/economic areas
Challenge format and depth	email to registered public contacts expecting human response (by email reply) within policy timeframe
Current phase	Completed, summary available
Summary or report	*Preliminary result: 82% prompt (1 working day) response, follow-up ongoing*

WISE, SIGISM, REFEDS, TI joint working group

see wise-community.org wiki and join!

https://wiki.geant.org/display/WISE/SCCC-JWG

co-chairs: Hannah Short (CERN) and David Groep (Nikhef)

Thank you

Any Questions?

davidg@nikhef.nl

AARC

https://aarc-community.org

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme and other sources.

This work is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-3).

We thank the following sources: EC Horizon 2020 projects GN4-3, EOSChub, and AARC-2; and the Dutch National e-Infrastructure coordinated by SURF