AARC Authentication and Authorisation for Research and Collaboration

Trust by Demonstration … in a coordinated way

Security Coordination Communications Challenges – all in it together

David Groep

AARC Community, policy and best practice area

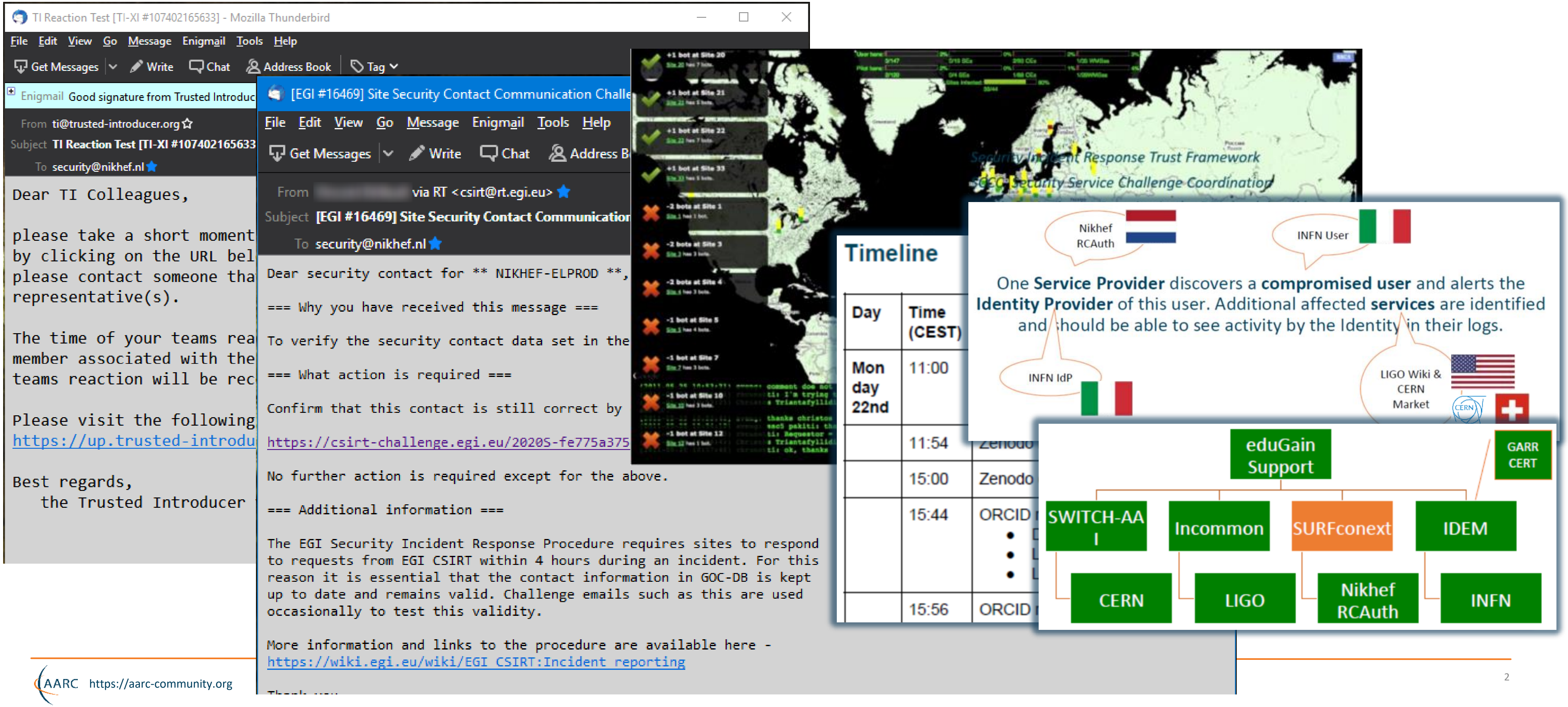
Nikhef PDP programme

Nikhef

WISE Community meeting

October 2021

Many communities test, test, and test again



TI Reaction Test [TI-XI #107402165633] - Mozilla Thunderbird
File Edit View Go Message Enigmail Tools Help
Get Messages Write Chat Address Book Tag
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
File Edit View Go Message Enigmail Tools Help
Get Messages Write Chat Address B

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
```

Timeline

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

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

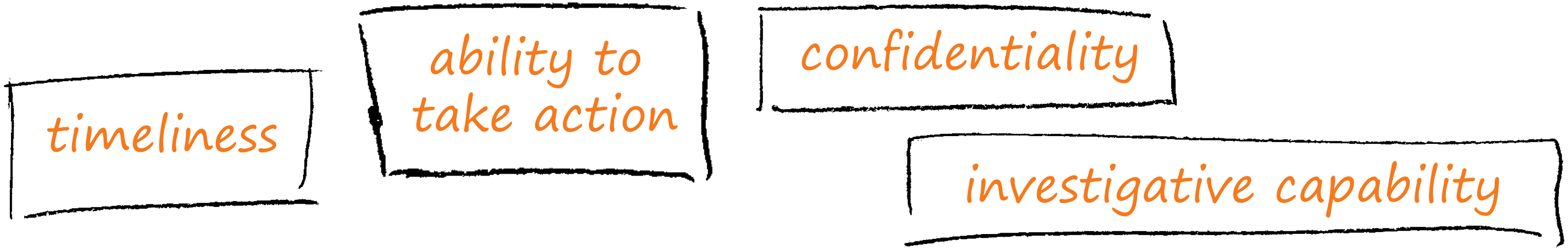
- every 1-2 years, in parallel with continuous operational monitoring

EGI CSIRT Security Service Challenges

- every ~2 years, aiming at remediation, forensics, and response to real-life (botnet) incidents

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

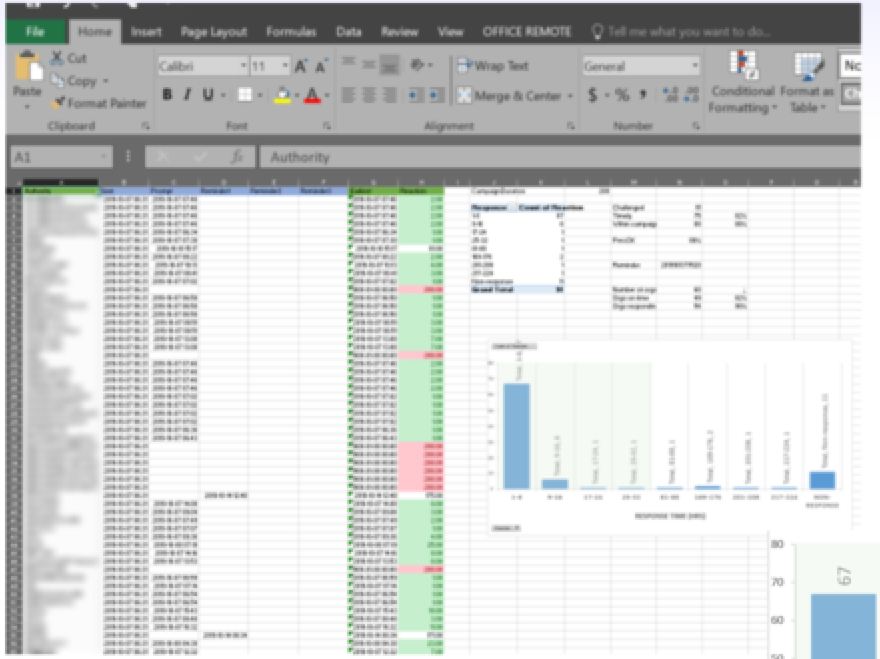
- when data available: infrastructure can set its *own level* of expectancy and gives *deep trust*
- assessment supported with community controls (suspension) gives a *baseline compliance*

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 …

IGFT RATCC4

IGTF RATCC4 Results



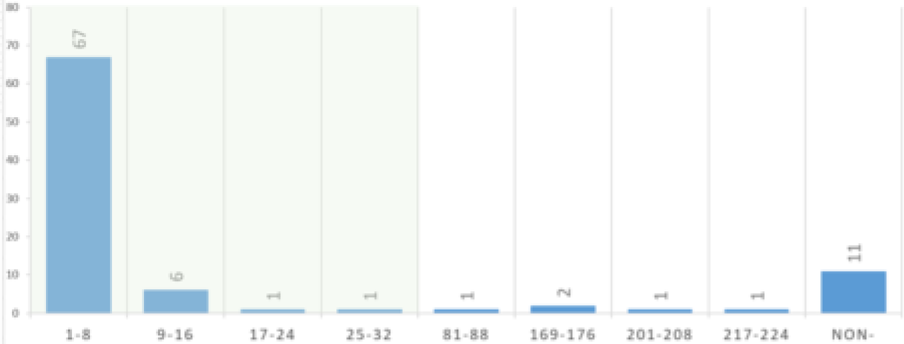
In total there are 91 trust anchors (root, intermediate, and issuing authorities) currently in the accredited bundle,

managed by 60 organisations.

Of the 60 organisations, 49 responded within one working day (82%), representing (incidentally) also 82% of the trust anchors.

Within a few days more, 3 additional ones came in, and 4 more responded after a reminder.

In total, 90% of the organisations responded to the challenge, representing 88% of the trust anchors.



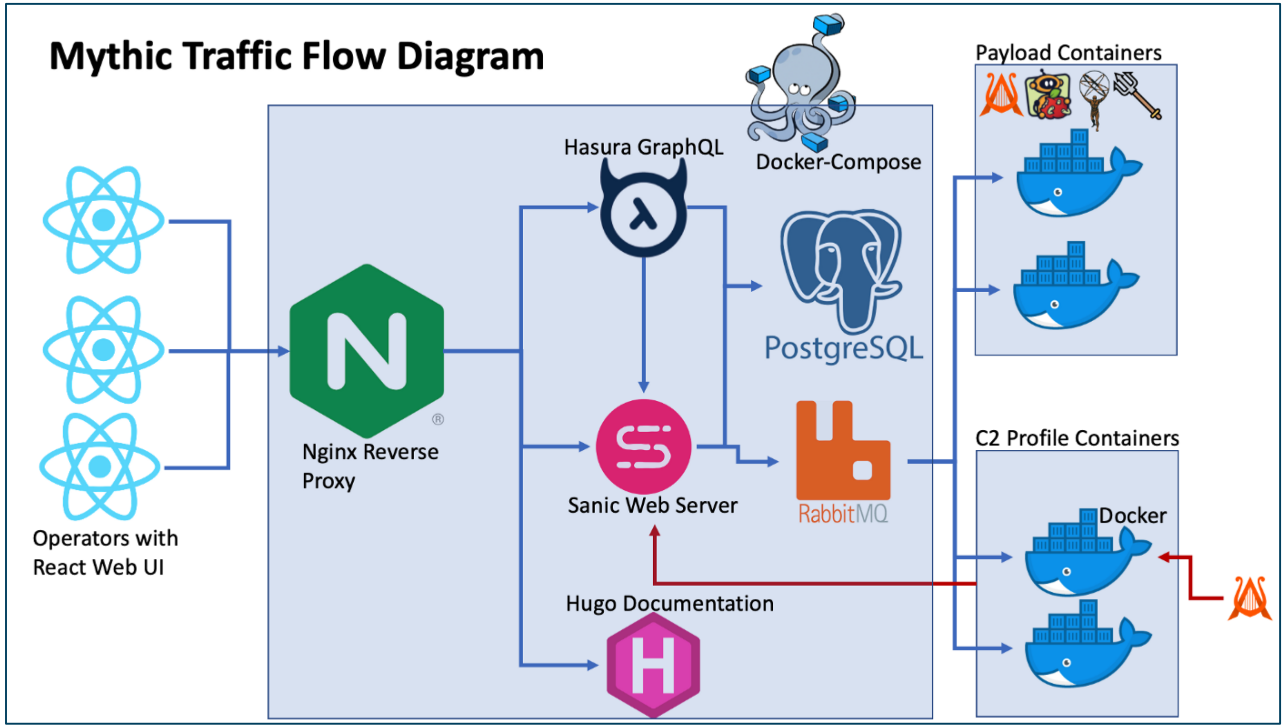
PS: of the non-response organisations,
4 had their public contact meta-data fixed, and 2 were withdrawn from the distribution

Upcoming EGI SSC challenge … simplified (with the Mythic C2)

- Many RedTeaming tools
  are now standard (like Mythic C2)

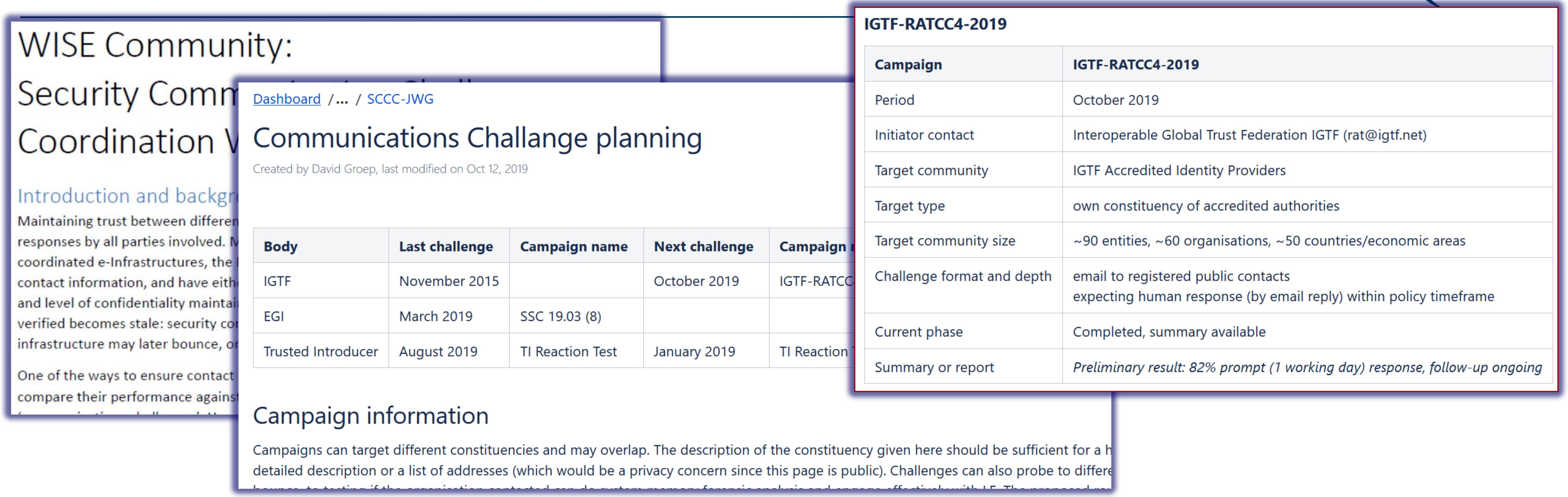
- containerisation aids in getting the payloads working across a heterogeneous infrastructure
  previous exercises ran into problems with the encrypted binaries and process hiding techniques

- integration with the operational submission systems remain
- as well as monitoring and report-out



https://docs.mythic-c2.net/
https://posts.specterops.io/learning-from-our-myths-45a19ad4d077

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 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 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 (GN4-2).

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

The SCCC Working Group – a joint effort of many

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 based on challenge frequency and results

- for example by specifying the level of disclosure detail for CCs
- as extension: could CCs be requested e.g. in response to changed risk assessments between infrastructures?

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 mail or click response consumes less resources than requesting forensics of simulated incident)

Frequency of CCs

- simple communications challenges are often performed one or several times per year
- 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