Authentication and Authorisation for Research and Collaboration

Trust by Demonstration … in a coordinated way

Security Coordination Communications Challenges – all in it together

David Groep
WISE SCCC-JWG & AARC Community,
Nikhef Physics Data Processing, UM Dept. of Advanced Computing Sciences

Nikhef Maastricht University

TNC22 Security Day - WISE Community
June 2022

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 Challenge -

File Edit View Go Message Enigmail Tools Help

Get Messages | Write | Chat | Address Book

From via RT <csirt@rt.egi.eu>

Subject [EGI #16469] Site Security Contact Communication Chall

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 GOC-

=== What action is required ===

Confirm that this contact is still correct by click

https://csirt-challenge.egi.eu/2020S-fe775a375ebe80db661e08d5ef602cc5ca5

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.

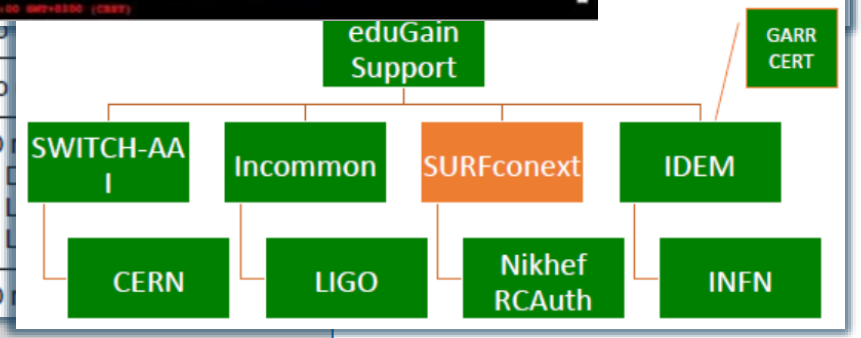
More information and links to the procedure are available here - https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting

Thank you

	11:54	Zenodo
	15:00	Zenodo
	15:44	ORCID
	15:56	ORCID

r and alerts the
vices are identified
in their logs.

Wiki &
ERN
arket



Not all tests are created equal … and not run equally either!

Trusted Introducer and TF-CSIRT

- ~3 Reaction Tests p/year, supported by web infrastructure, (team) authenticated responses

SURFcert challenges for the national (federated) contacts

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

Communications Challenges: IGTF RAT, eduGAIN-to-federation-ops, EOSC Core providers …

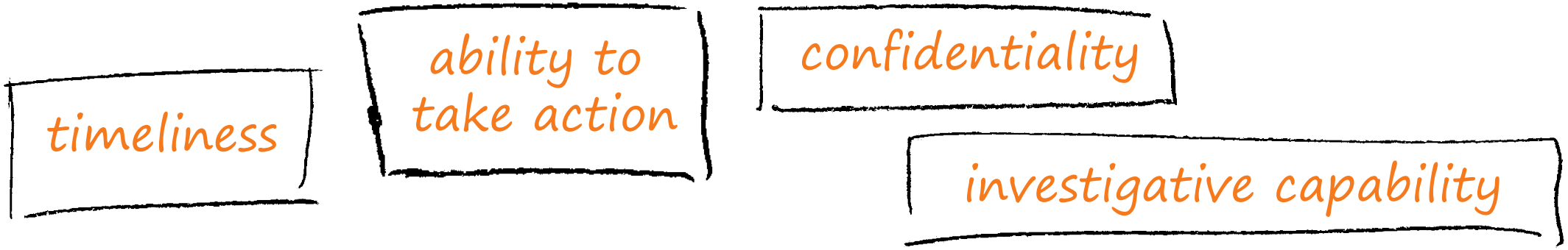
- periodic, from every 1-2 years, to annualy
- usually in parallel with continuous operational monitoring

EGI CSIRT Security Service Challenges

- every ~2 years, aiming at remediation, forensics, and response to real-life (botnet) incidents
- requires much more preparation, and integration with research workflow systems costly

Challenge elements – what is valued or expected might differ …

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



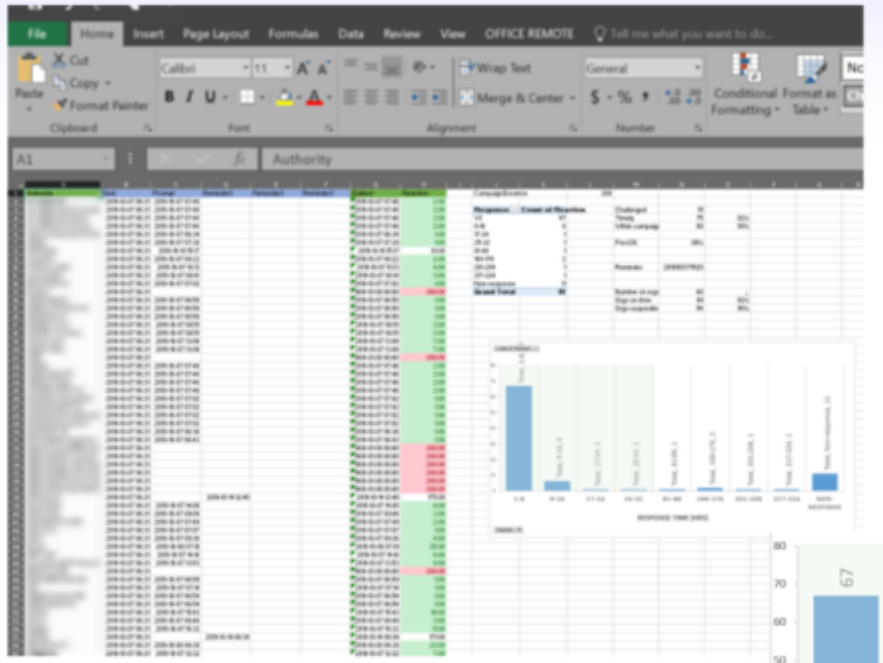
- when data available: infrastructure can set its *own level* of expectancy and gives *deep trust*
- assessment supported with community controls (even suspension) gives a *baseline compliance*

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



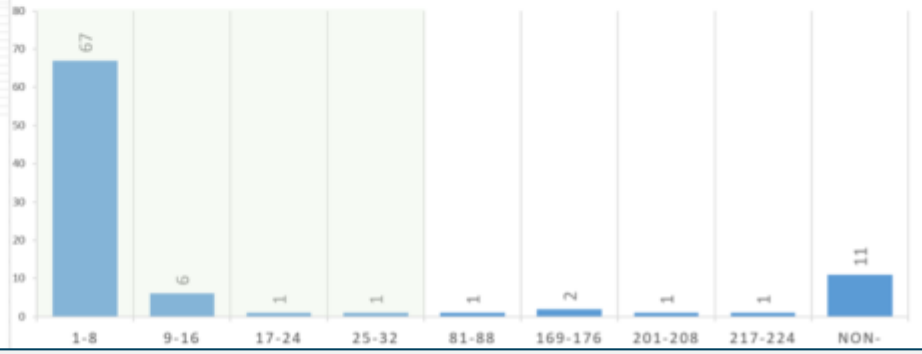
In total there are 91 trust anchors (root, intermediate, and issuing authorities) currently in the accredited bundle,

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

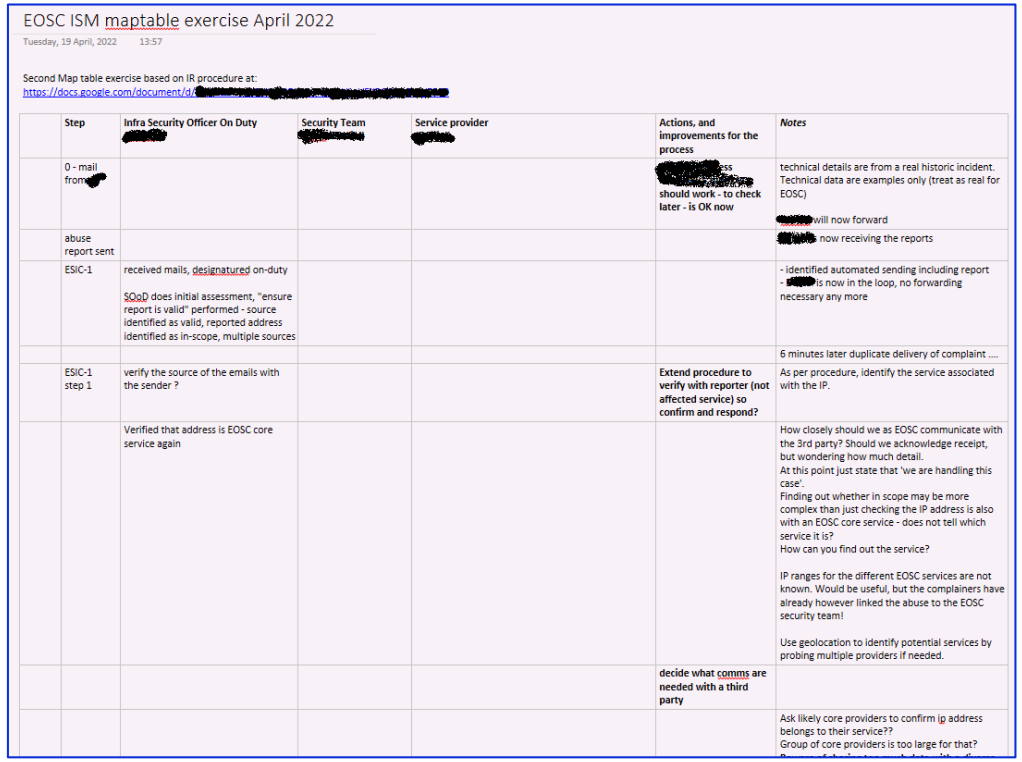
Designing challenges for new targets: the European Open Science Cloud

Distance between operational security and (exchange) services remains large

- *who to target first in an open ecosystem?*
- *raising awareness as well as improving response*

Core services easier to identify

- security contact are in place
- service management system is known
- on-boarding process being rolled out



EOSC ISM maptable exercise April 2022

Tuesday, 19 April, 2022 13:57

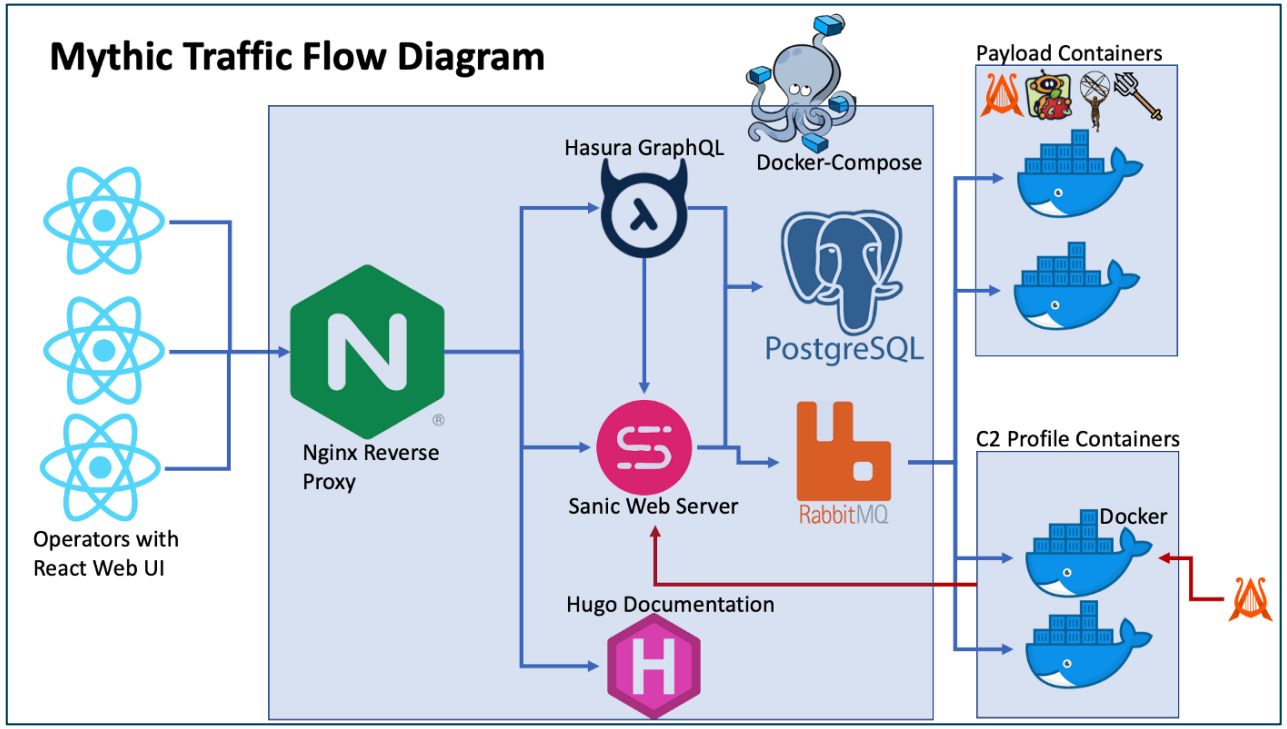
Second Map table exercise based on IR procedure at:
https://docs.google.com/document/d/[redacted]

	Step	Infra Security Officer On Duty [redacted]	Security Team [redacted]	Service provider [redacted]	Actions, and improvements for the process	Notes
	0 - mail from [redacted]				[redacted] should work - to check later - is OK now	technical details are from a real historic incident. Technical data are examples only (treat as real for EOSC) [redacted] will now forward
	abuse report sent					[redacted] now receiving the reports
	ESIC-1	received mails, designatured on-duty SOoD does initial assessment, "ensure report is valid" performed - source identified as valid, reported address identified as in-scope, multiple sources				- identified automated sending including report - [redacted] is now in the loop, no forwarding necessary any more
						6 minutes later duplicate delivery of complaint ....
	ESIC-1 step 1	verify the source of the emails with the sender ?			Extend procedure to verify with reporter (not affected service) so confirm and respond?	As per procedure, identify the service associated with the IP.
		Verified that address is EOSC core service again				How closely should we as EOSC communicate with the 3rd party? Should we acknowledge receipt, but wondering how much detail. At this point just state that 'we are handling this case'. Finding out whether in scope may be more complex than just checking the IP address is also with an EOSC core service - does not tell which service it is? How can you find out the service? IP ranges for the different EOSC services are not known. Would be useful, but the complainers have already however linked the abuse to the EOSC security team! Use geolocation to identify potential services by probing multiple providers if needed.
					decide what comms are needed with a third party	
						Ask likely core providers to confirm ip address belongs to their service?? Group of core providers is too large for that?

- **but designing the security scenarios is an art in itself (thanks to Pinja Koskinen and Alf Moens!)**

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

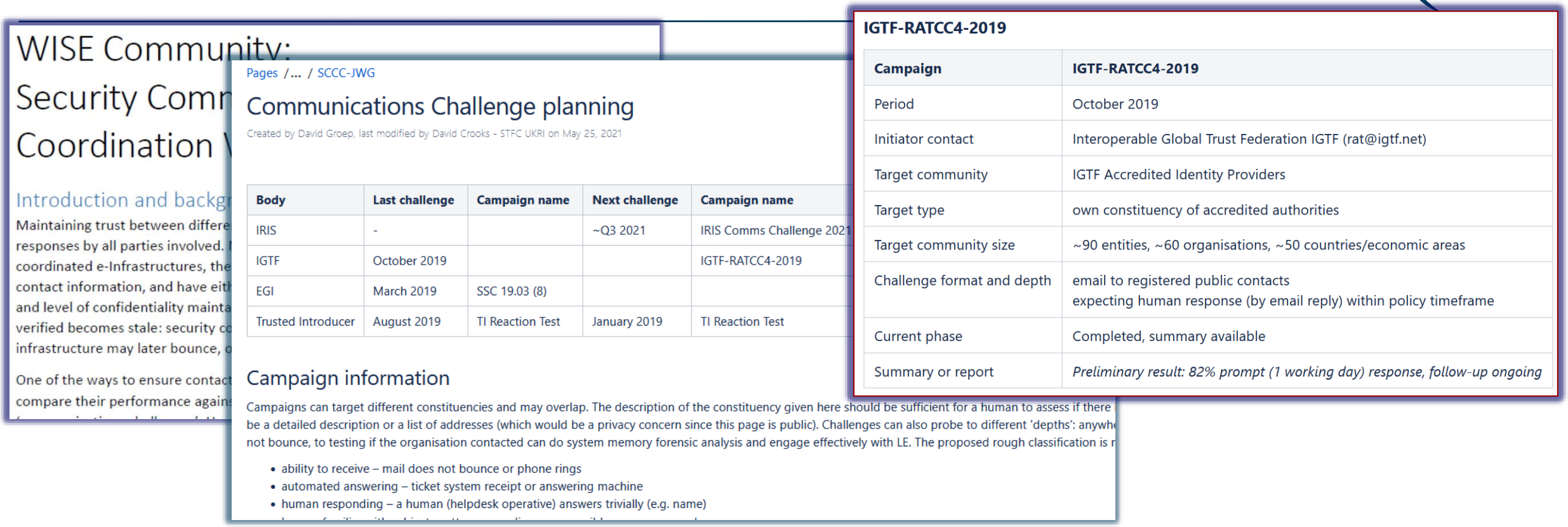


https://docs.mythic-c2.net/
https://posts.specterops.io/learning-from-our-myths-45a19ad4d077

Designing forestics-oriented challenges is exhilarating in itself

imagery: SSC5 Oscar Koeroo, Graeme Stuart, EGI CSIRT team, WLCG, *et al.*

WISE SCCC-WG – participate!



WISE Community:
Security Comm
Coordination

Introduction and backgr
Maintaining trust between differe
responses by all parties involved.
coordinated e-Infrastructures, the
contact information, and have eith
and level of confidentiality mainta
verified becomes stale: security c
infrastructure may later bounce,

One of the ways to ensure contact
compare their performance agains

Pages / ... / SCCC-JWG

Communications Challenge planning

Created by David Groep, last modified by David Crooks - STFC UKRI on May 25, 2021

Body	Last challenge	Campaign name	Next challenge	Campaign name
IRIS	-		~Q3 2021	IRIS Comms Challenge 2021
IGTF	October 2019			IGTF-RATCC4-2019
EGI	March 2019	SSC 19.03 (8)		
Trusted Introducer	August 2019	TI Reaction Test	January 2019	TI Reaction Test

Campaign information

Campaigns can target different constituencies and may overlap. The description of the constituency given here should be sufficient for a human to assess if there
be a detailed description or a list of addresses (which would be a privacy concern since this page is public). Challenges can also probe to different 'depths': anywh
not bounce, to testing if the organisation contacted can do system memory forensic analysis and engage effectively with LE. The proposed rough classification is

- ability to receive – mail does not bounce or phone rings
- automated answering – ticket system receipt or answering machine
- human responding – a human (helpdesk operative) answers trivially (e.g. name)

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)

Making the SCCC JWG a useful place for all

- How to grow the community and leverage the trust built?
- Can we use joint machinery for running challenges?
  eduGAIN, EGI, TI, SURF all have tooling, and more is coming
- The Wiki page is a start – evolution and completeness requires *you*!

Thank you

Any Questions?

davidg@nikhef.nl

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