Communications Challenge planning

Body	Last challenge	Campaign name	Next challenge	Campaign name	Status
IGTF	October 2019			IGTF-RATCC4-2019	Completed
EGI	March 2019	SSC 19.03 (8)			(Completed
Trusted Introducer	August 2019	TI Reaction Test	January 2019	TI Reaction Test	Repeats three times a year

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 is a significant overlap in community, it need not 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': anywhere from just checking if a contact address does not bounce, to testing if the organisation contacted can do system memory forensic analysis and engage effectively with LE. The proposed rough classification is now:

- 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)
- human familiar with subject-matter responding – responsible person responds
- service analysis capability - a responsible person or team can investigate and resolve common incidents reported to the contact address (forensics, log processing, &c)

See also https://www.eugridpma.org/agenda/47/contribution/6/material/slides/0.pptx for some background.

Please **do not post sensitive data** to this Wiki - it is publicly viewable for now.

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*

EGI Security Service Challenge 6 (19.03)

Campaign	EGI-SSC-19.03 (8)
Period	March 2019us
Initiator contact	EGI CSIRT (csirt@mailman.egi.eu)
Target community	EGI Federation members: service providers and selected user communities
Target type	own constituency of service providers
Target community size	~70 organisations, ~14 countries/IOs
Challenge format and depth	simulated user-level system intrusion using (non-weaponized) crafted malware expecting communications with federation CSIRT, log analysis and correlation, and forensic investigation should follow established procedures and communications reponse deadlines
Current phase	Completed

Summary or report	*summary available upon request* *description of challenge format and malware publicly available: https://indico.cern.ch/event/739878/contributions/3380156/attachments/1840866/3018165/gdb-20190508.pdf*

TI Reaction Test

Campaign	TI Reaction Test
Period	August 2019
Initiator contact	Trusted Introducer Team (ti@trusted-introducer.org)
Target community	TI Listed, Accredited and Certified Teams
Target type	R&E, military, commercial, government, e-infrastructure and national certs as per participation in TI.
Target community size	363 teams (as at August 2019)
Challenge format and depth	Simple click link response to show that team has ability to respond quickly. Team must have valid certificate to complete the response.
Current phase	Completed
Summary or report	*Results are available for participating teams only at: https://tiw.trusted-introducer.org/news/reaction-tests.html.*