

Information Security 3: Who you gonna call?

David Groep

Security Coordination Group
AARC Policy & Best Practice coordination, EOSCHUB ISM, GN4 EnCo, SURF DNI
Nikhef Physics Data Processing group

Nikhef



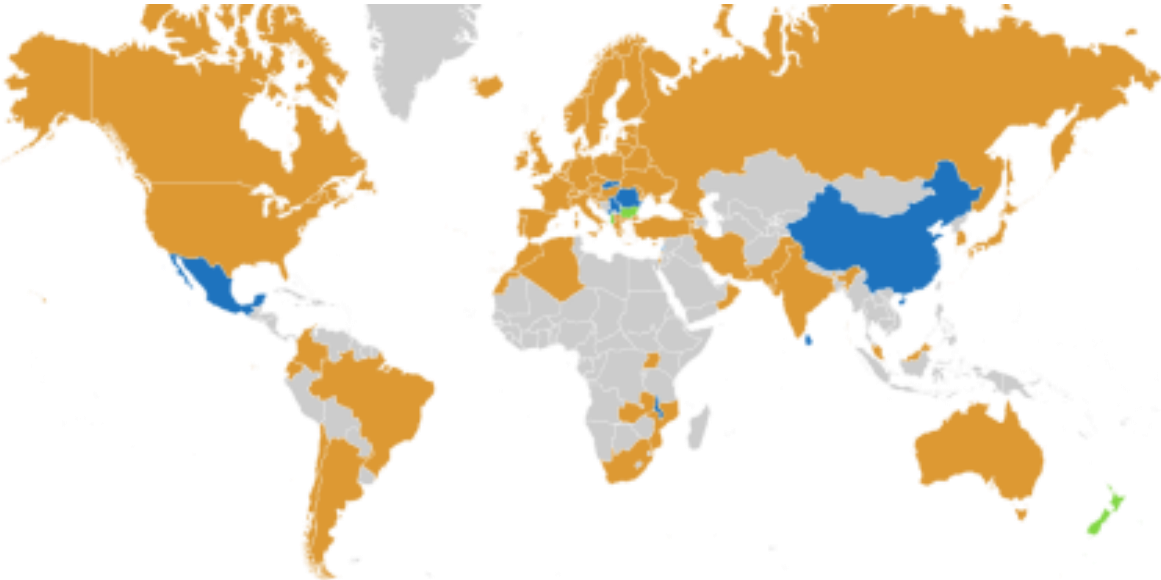
www.egi.eu

*In collaboration with & co-supported
by AARC – aarc-project.eu*

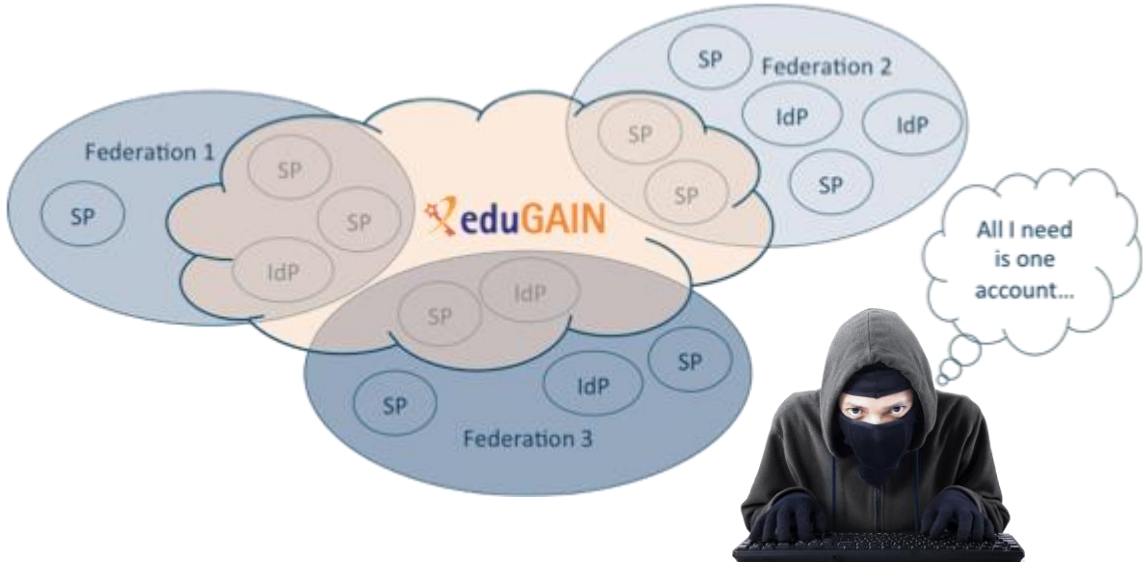


R&E federation and eduGAIN – and the wonderful world of this session

eduGAIN – many countries & economic regions with an R&E identity federation



... yet incident response has to be global (since the miscreants certainly are ☹) ...



full of valuable resources (data, network, services)



Incidents spread through the community

We live & breath federation!

- communities have access to services in many sites, in countries across the globe,
- which is anyway better than before federated login, where users had accounts (all with the same password) everywhere,
- but the spread of incidents, and finding good targets, remains as easy as it ever was!

The broader view



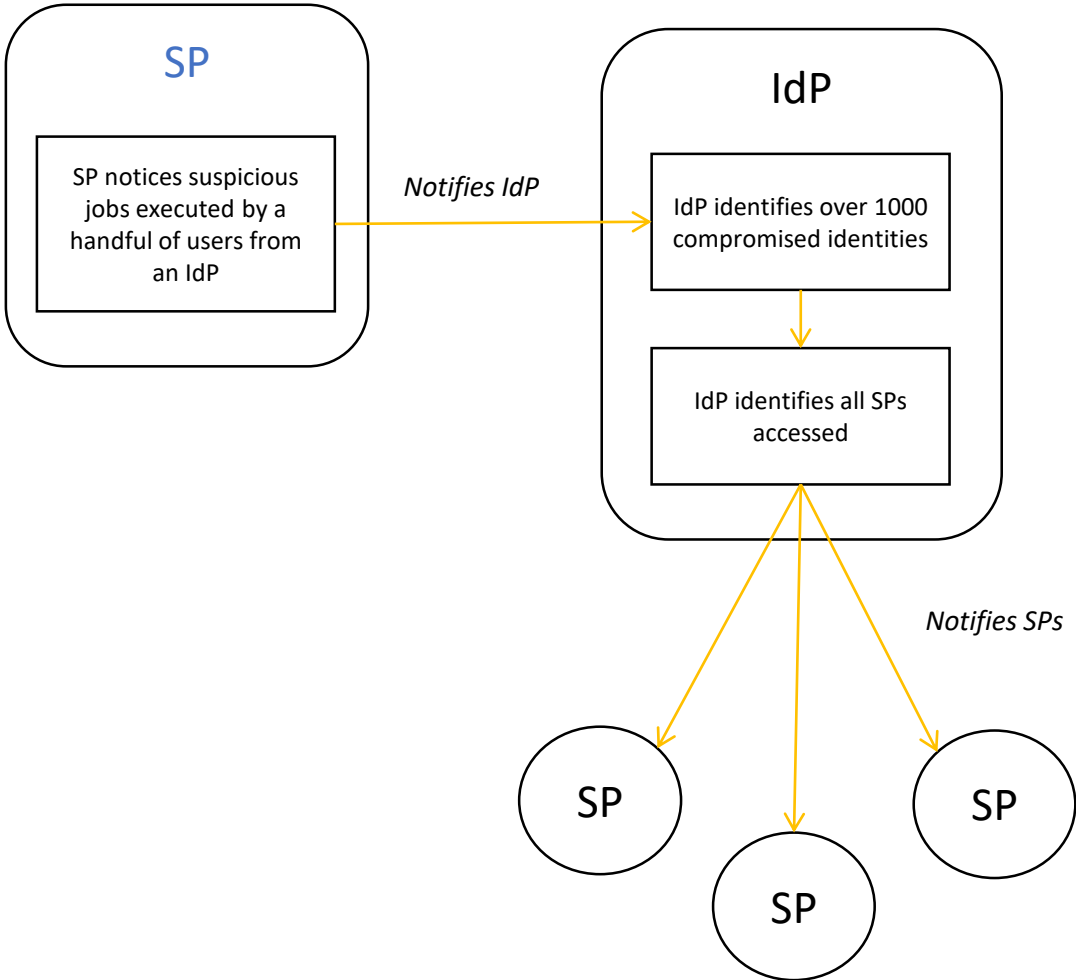
Some of the sites/companies/providers known to have been at the receiving end of an attack:

berkeley.edu	gatech.edu	rr.com	ucsc.edu
bonet.se	iastate.edu	rutgers.edu	ucsd.edu
brandeis.edu	jhu.edu	sdsc.edu	uiuc.edu
bredbandsbolaget.se	ki.se	seagull.net	umea.se
brown.edu	kralovopolska.cz	simons-rock.edu	umearc.se
bu.edu	kth.se	skanova.com	umn.edu
cam.ac.uk	liu.se	skogsbrynet.se	umu.se
cern.ch	liv.ac.uk	songnetworks.se	unige.ch
chalmers.se	lu.se	stanford.edu	uta.fi
cisco.com	mit.edu	technion.ac.il	utk.edu
columbia.edu	naqua.se	telia.com	uu.se
csbnet.se	nasa.gov	uchicago.edu	wsmr.army.mil
desy.de	nikhef.nl	uci.edu	
epfl.ch	pitt.edu	ucolorado.edu	

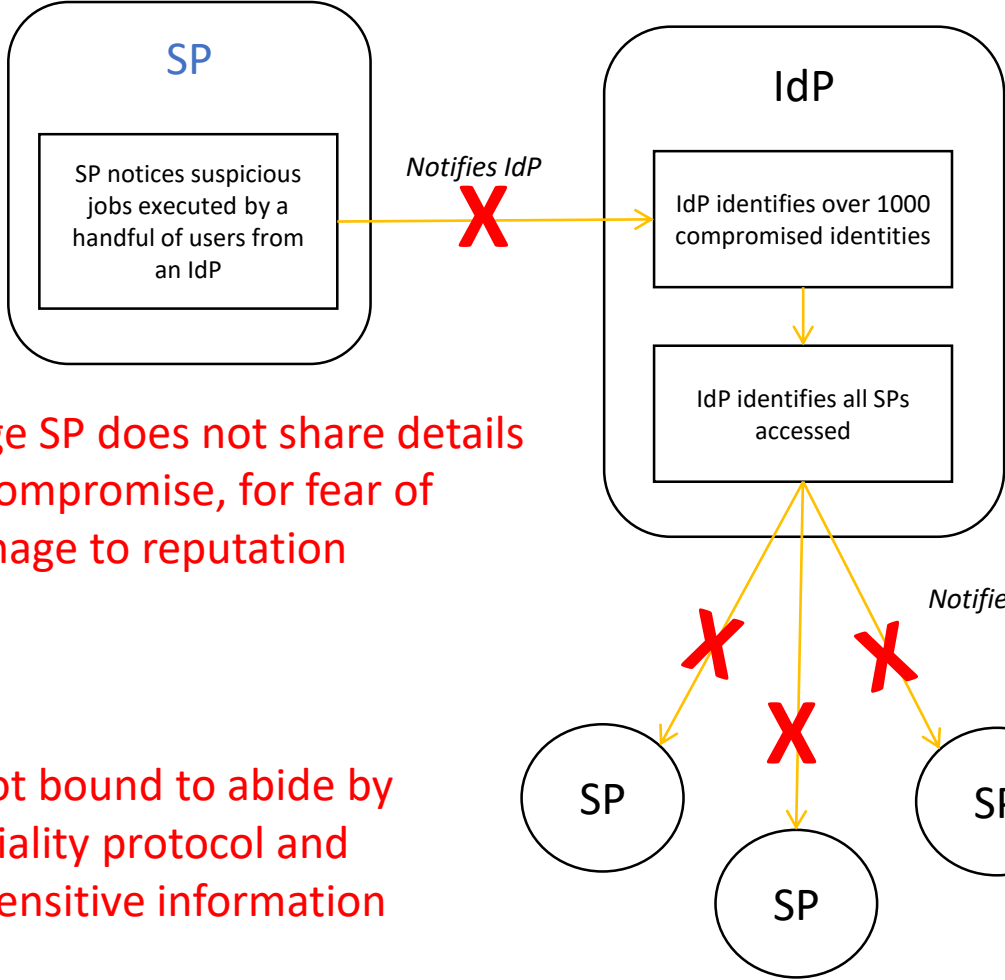
This is just a small sample; from August 2003 through March 2005 something like a thousand sites were attacked.

slide with site names: Stakkato incident – investigation by Leif Nixon 13/57

But what appears trivial



... may not be so ...



Small IdP may not have capability to block users, or trace their usage



Large SP does not share details of compromise, for fear of damage to reputation



SPs are not bound to abide by confidentiality protocol and disclose sensitive information

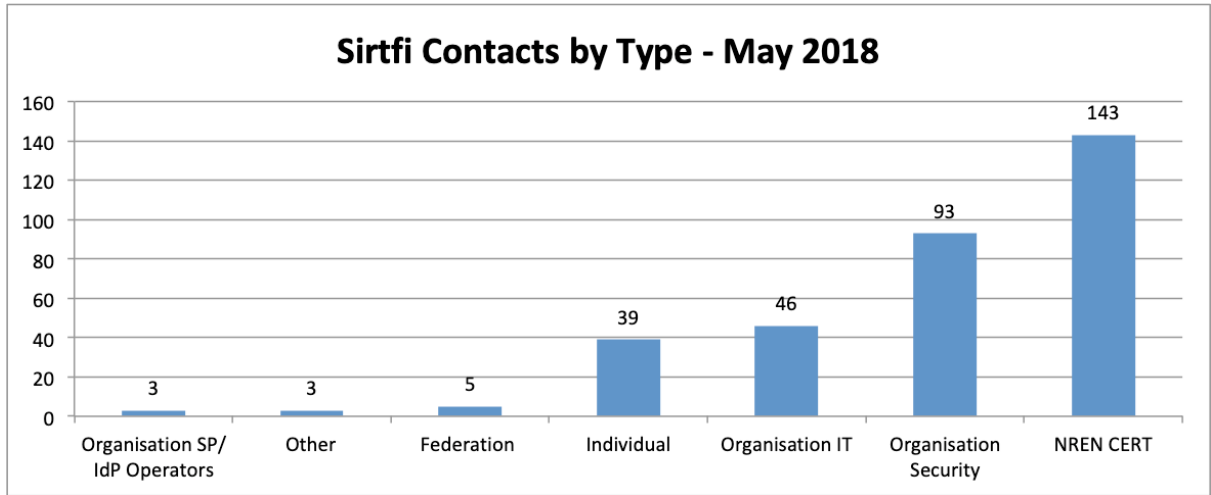
No security contact details!



So who do *you* call?

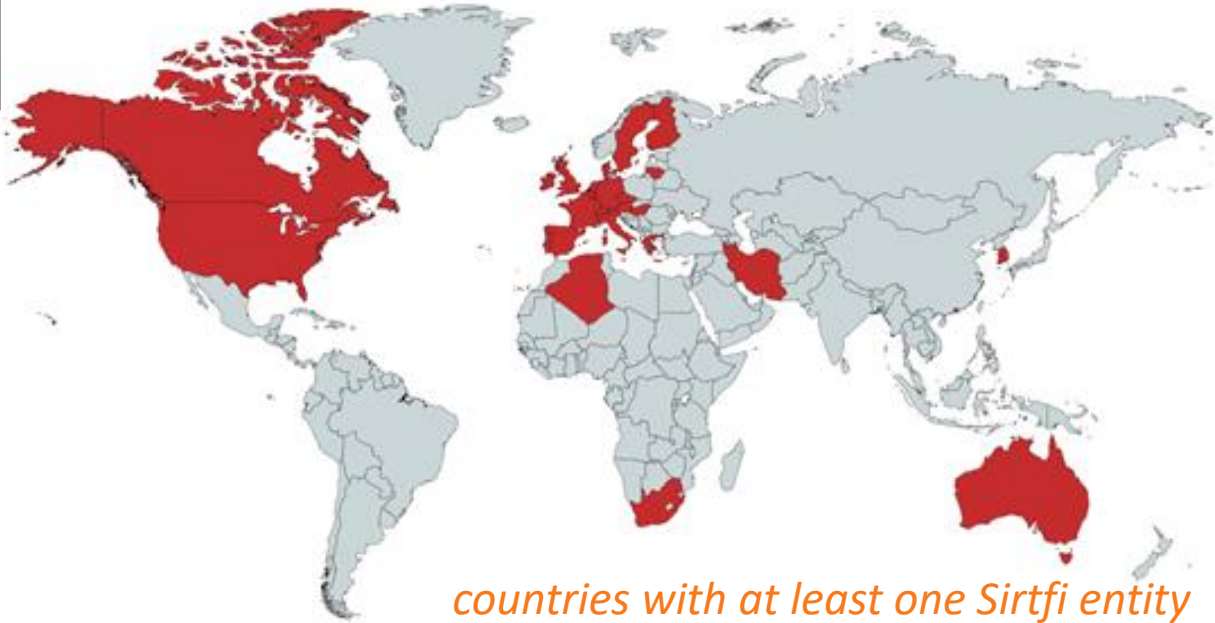
- Do you follow only the network?
 - WHOIS data, abuse contacts in RIPPEDB, and ... pray
- **Or:** do you follow the community?
 - look at authorization log and find the community contact in the VOID card
 - community will have to look for the user, meanwhile the incident goes on
- **and** do you contact your peers?
 - call EGI CSIRT (always a good idea) and share IoCs to protect likely victims
- **and** do you contact the identity provider mitigate issue at source?
 - use federation meta-data to find a trusted contact point with *Sirtfi*
 - involve the eduGAIN support desk security function to get global reach

Sirtfi is there today – 561 parties joined, in 28 federations



Incident Response

- Assure confidentiality of information exchanged
- Identify trusted contacts
- Guarantee a response during collaboration



countries with at least one Sirtfi entity

IAM Online Europe

IAM Online Europe webinars are brought to you by AARC



iamonlineEU 001 Sirtfi
iamOnline
38 views • 4 days ago

<https://refeds.org/SIRTFI> REFEDS > SIRTFI

Incident Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response organisations. This assurance framework comprises a list of assertions which an organisation can attest in order to be compliant. Visit our [Wiki](#) to discover how your organisation can prepare itself for Federated Incident Response.

The AARC Group has been active since 2014 and combines expertise in operational security and incident response policies. Work to publish and implement the Sirtfi Trust Framework is supported by the AARC community.



Benefits



Sirtfi v 1.0



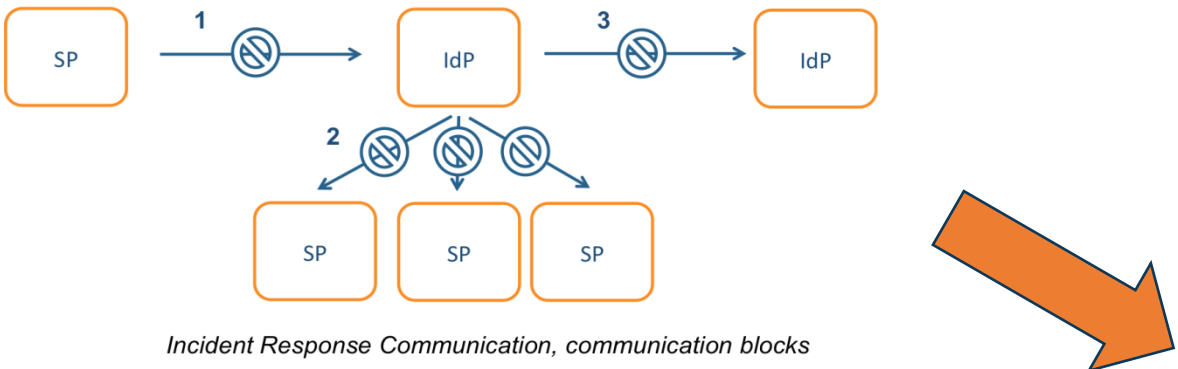
FAQs

[AARC https://aarc.org](https://aarc.org) Why should I join? What are the Benefits?

[View the Sirtfi Framework](#)

[Need help?](#)

Incident response process evolution in federations



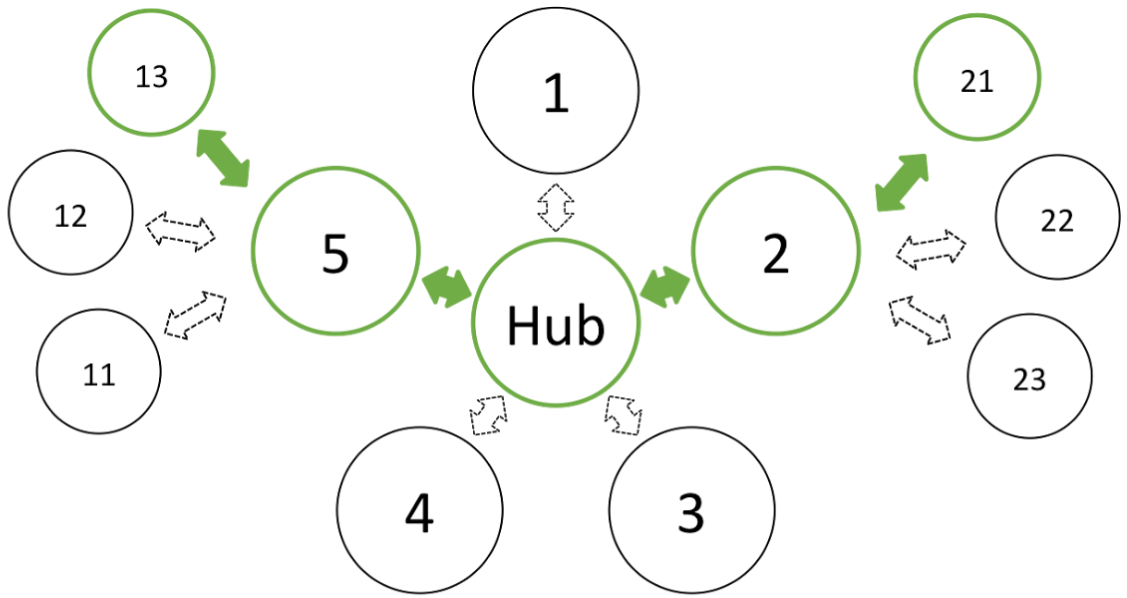
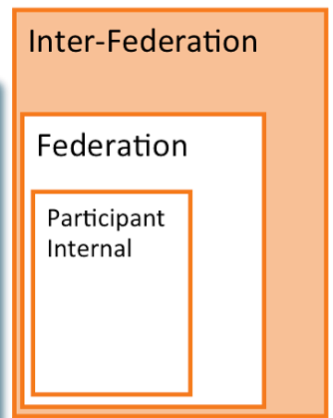
Proposed solutions

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

Guide to Federated Security Incident Response for Research Collaboration



Publication Date: 2019-03-22
 Authors: Hannah Short; David Groep; AARC NA3
 Document Code: AARC-I051

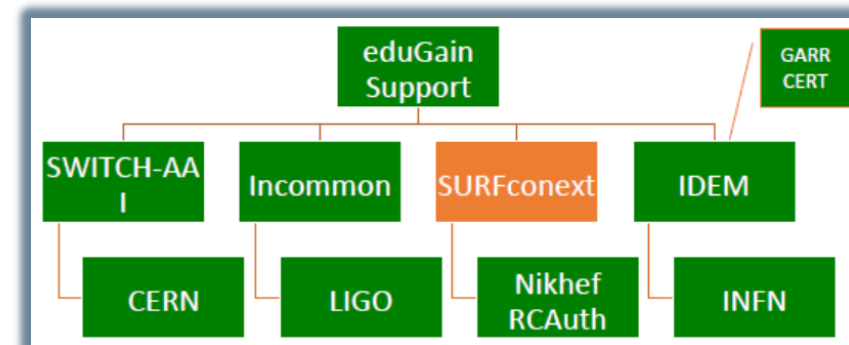
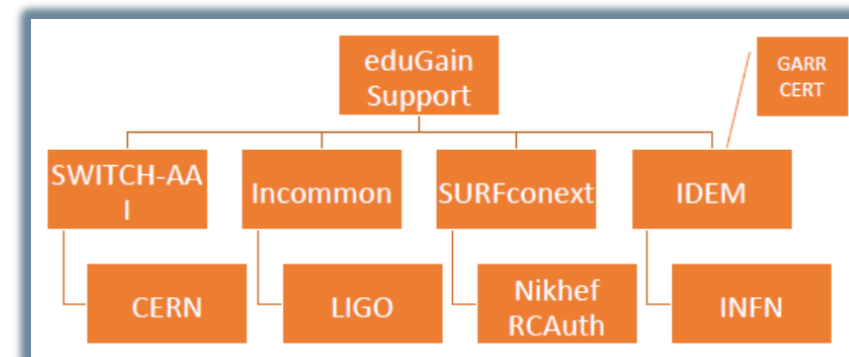


Inter-Federation Incident Response Communication

Test model for federated incident response

- defines the model actors in a global test incident
- include eduGAIN Support Desk
- exercise the attack scenario!

and learn: the result is AARC-I051 with a reference process



parties involved in response challenge

Report-out see <https://wiki.geant.org/display/AARC/Incident+Response+Test+Model+for+Organizations>

Trusted Introducer and TF-CSIRT

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

Nationally, e.g. the 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

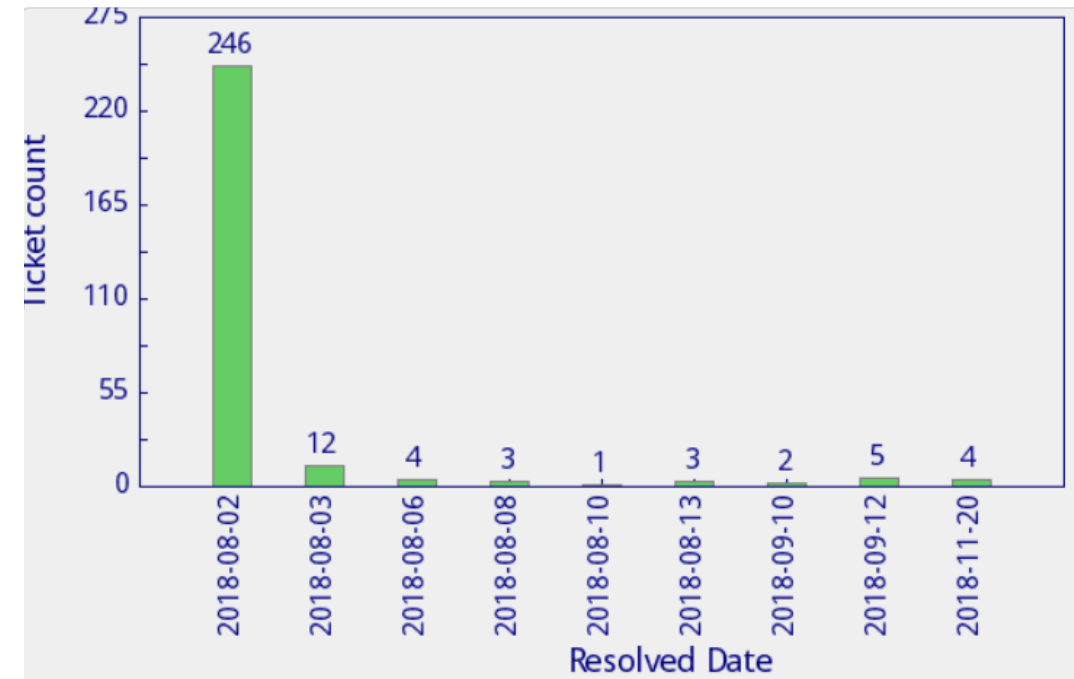
EGI CSIRT: both comms challenges and security service challenges

- are the contacts in GOCDDB correct and responsive?
- do the service providers know what to do if a real incident strikes?

Communication Challenge 2018 Results

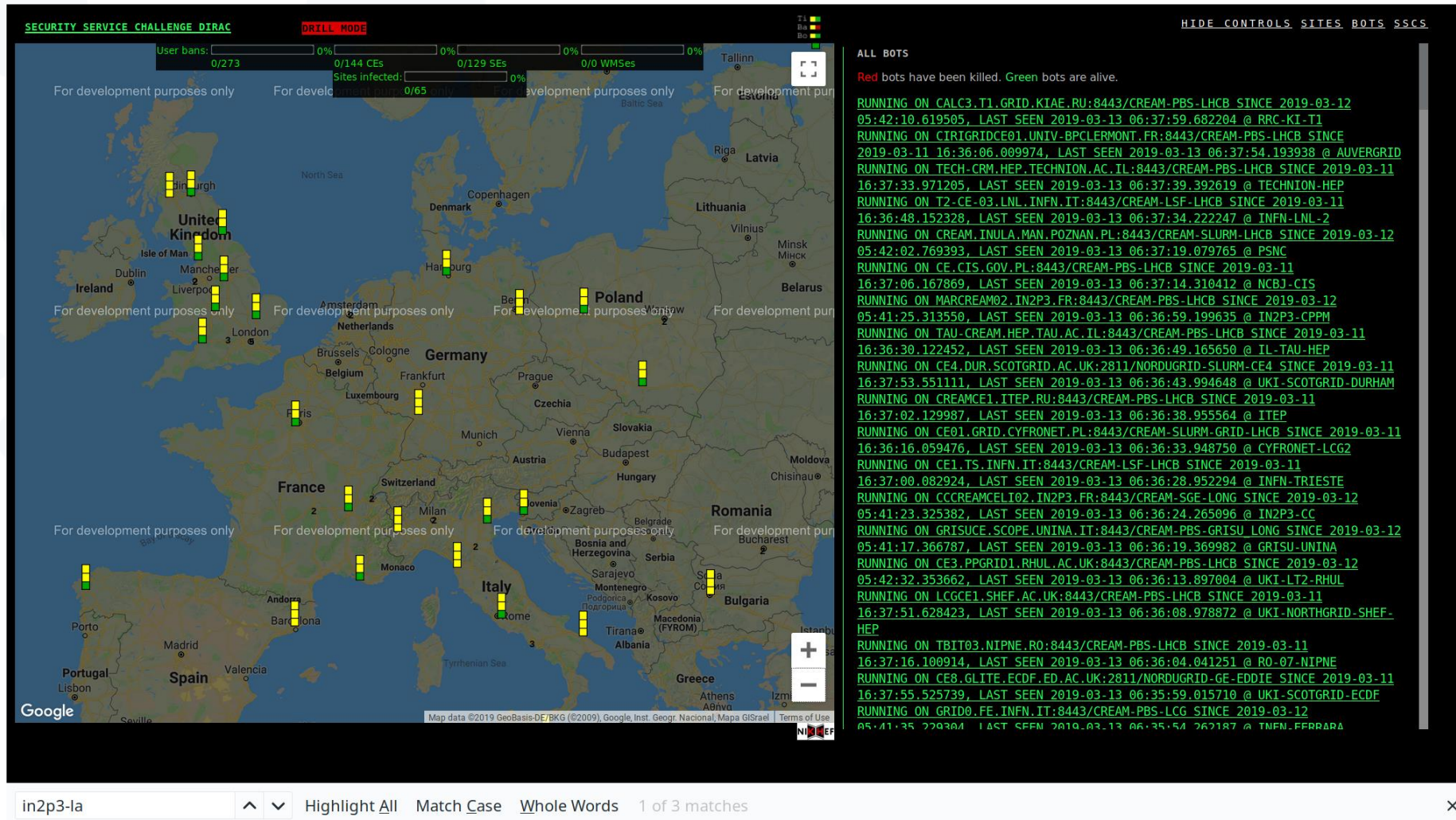
- 23/272 clicks within 1 minute (8%)
- 101/272 clicks within 10 minutes (37%)
- 179/272 clicks within 1 hour (66%)
- **214/272 clicks within 4 hours (79%)**
- 234/272 clicks within 1 day (86%)
- 252/272 clicks within 4 days (93%)
- 261/272 clicks within 7+ days (96%)
- 2 clicks at 39 days...
- 9 without direct clicks

Working-hour wise, these numbers are even better!



data and imagery: Sven Gabriel, EGI CSIRT presentation ISGC 2019

Can a coordinated service provider federation do better?



The screenshot displays a security dashboard with a map of Europe and a list of bot activity logs. The map shows various countries with green and red markers indicating bot locations. The dashboard includes statistics for user bans, sites infected, and development purposes. The bot activity log lists running bots with their IP addresses, last seen times, and locations.

SECURITY SERVICE CHALLENGE DIRAC **DRILL MODE**

User bans: 0/273 (0%)
 Sites infected: 0/144 (0%)
 Development purposes only: 0/129 (0%)
 WMSes: 0/0 (0%)

ALL BOTS
 Red bots have been killed. Green bots are alive.

Running bots (examples):

- `RUNNING ON CALC3.T1.GRID.KIAE.RU:8443/CREAM-PBS-LHCB SINCE 2019-03-12 05:42:10.619505, LAST SEEN 2019-03-13 06:37:59.682204 @ RRC-KI-T1`
- `RUNNING ON CIRIGRIDCE01.UNIV-BPCLERMONT.FR:8443/CREAM-PBS-LHCB SINCE 2019-03-11 16:36:06.009974, LAST SEEN 2019-03-13 06:37:54.193938 @ AUVERGRID`
- `RUNNING ON TECH-CRM.HEP.TECHNION.AC.IL:8443/CREAM-PBS-LHCB SINCE 2019-03-11 16:37:33.971205, LAST SEEN 2019-03-13 06:37:39.392619 @ TECHNION-HEP`
- `RUNNING ON T2-CE-03.LNL.INFN.IT:8443/CREAM-LSF-LHCB SINCE 2019-03-11 16:36:48.152328, LAST SEEN 2019-03-13 06:37:34.222247 @ INFN-LNL-2`
- `RUNNING ON CREAM.INULA.MAN.POZNAK.PL:8443/CREAM-SLURM-LHCB SINCE 2019-03-12 05:42:02.769393, LAST SEEN 2019-03-13 06:37:19.079765 @ PSNC`
- `RUNNING ON CE.CIS.GOV.PL:8443/CREAM-PBS-LHCB SINCE 2019-03-11 16:37:06.167869, LAST SEEN 2019-03-13 06:37:14.310412 @ NCBJ-CIS`
- `RUNNING ON MARCREAM02.IN2P3.FR:8443/CREAM-PBS-LHCB SINCE 2019-03-12 05:41:25.313550, LAST SEEN 2019-03-13 06:36:59.199635 @ IN2P3-CPPM`
- `RUNNING ON TAU-CREAM.HEP.TAU.AC.IL:8443/CREAM-PBS-LHCB SINCE 2019-03-11 16:36:30.122452, LAST SEEN 2019-03-13 06:36:49.165650 @ IL-TAU-HEP`
- `RUNNING ON CE4.DUR.SCOTGRID.AC.UK:2811/NORDUGRID-SLURM-CE4 SINCE 2019-03-11 16:37:53.551111, LAST SEEN 2019-03-13 06:36:43.994648 @ UKI-SCOTGRID-DURHAM`
- `RUNNING ON CREAMCE1.ITEP.RU:8443/CREAM-PBS-LHCB SINCE 2019-03-11 16:37:02.129987, LAST SEEN 2019-03-13 06:36:38.955564 @ ITEP`
- `RUNNING ON CE01.GRID.CYFRONET.PL:8443/CREAM-SLURM-GRID-LHCB SINCE 2019-03-11 16:36:16.059476, LAST SEEN 2019-03-13 06:36:33.948750 @ CYFRONET-LCG2`
- `RUNNING ON CE1.TS.INFN.IT:8443/CREAM-LSF-LHCB SINCE 2019-03-11 16:37:00.082924, LAST SEEN 2019-03-13 06:36:28.952294 @ INFN-TRIESTE`
- `RUNNING ON CCCREAMCELI02.IN2P3.FR:8443/CREAM-SGE-LONG SINCE 2019-03-12 05:41:23.325382, LAST SEEN 2019-03-13 06:36:24.265096 @ IN2P3-CC`
- `RUNNING ON GRISUCE.SCOPE.UNINA.IT:8443/CREAM-PBS-GRISU LONG SINCE 2019-03-12 05:41:17.366787, LAST SEEN 2019-03-13 06:36:19.369982 @ GRISU-UNINA`
- `RUNNING ON CE3.PPGRID1.RHUL.AC.UK:8443/CREAM-PBS-LHCB SINCE 2019-03-12 05:42:32.353662, LAST SEEN 2019-03-13 06:36:13.897004 @ UKI-LT2-RHUL`
- `RUNNING ON LCGCE1.SHEP.AC.UK:8443/CREAM-PBS-LHCB SINCE 2019-03-11 16:37:51.628423, LAST SEEN 2019-03-13 06:36:08.978872 @ UKI-NORTHGRID-SHEP-HEP`
- `RUNNING ON TBIT03.NIPNE.RO:8443/CREAM-PBS-LHCB SINCE 2019-03-11 16:37:16.100914, LAST SEEN 2019-03-13 06:36:04.041251 @ RO-07-NIPNE`
- `RUNNING ON CE8.GLITE.ECDF.ED.AC.UK:2811/NORDUGRID-GE-EDDIE SINCE 2019-03-11 16:37:55.525739, LAST SEEN 2019-03-13 06:35:59.015710 @ UKI-SCOTGRID-ECDF`
- `RUNNING ON GRID0.FE.INFN.IT:8443/CREAM-PBS-LCG SINCE 2019-03-12 05:41:35.229304, LAST SEEN 2019-03-13 06:35:54.262187 @ INFN-FERRARA`

Search: in2p3-la | Highlight All | Match Case | Whole Words | 1 of 3 matches

Go to the Tuesday morning security session to find out!

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

will be a **joint** working group by WISE, SIG-ISM, REFEDS, and the IGTF

Let's communicate!
wise-community.org
aarc-project.eu
csirt.egi.eu
technical.edugain.org



www.egi.eu



AARC elements © GÉANT on behalf of the AARC project. AARC material licensed under a Creative Common Attribution 4.0 (CC-BY) License. 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).

Elements by EGI.eu licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

David Groep
davidg@nikhef.nl
<https://www.nikhef.nl/~davidg/presentations/>
 <https://orcid.org/0000-0003-1026-6606>