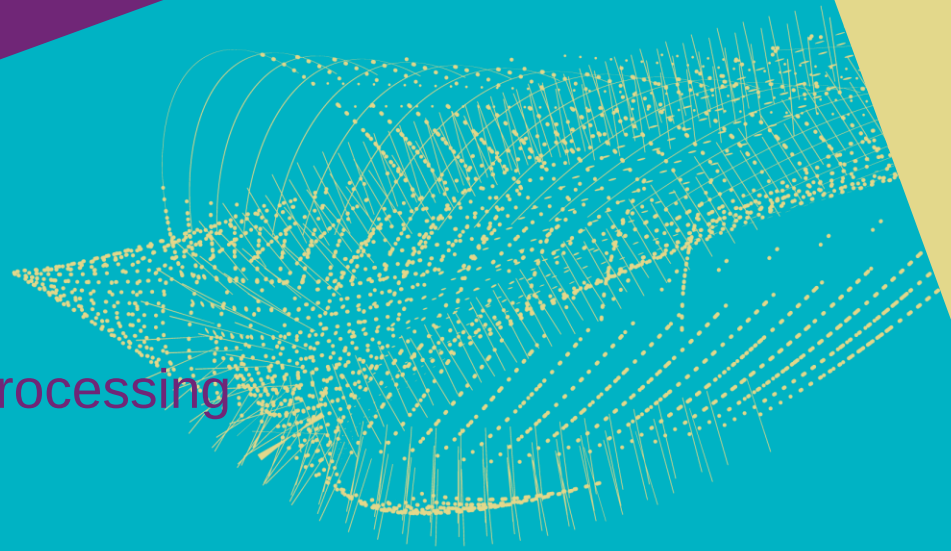
Nikhef



David Groep, Physics Data Processing

Staying reasonably safe in an open research environment

August 2020
updated December 2020
for the NWO-I IT managers meeting

Did anyone attend - or watch - the UM symposium?

You should! It's a great resource and excellent example of how to deal with a case like this well

https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt

What is worthy of your protection?

What's the risk & what's at stake

Protection measures

prevention

preparing for commensurate response

Since it will happen …

your local security capability

analytics & sharing intelligence,

communication and exercises

Finally it did happen – and now what?

From Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners; Jason Andress, Steve Winterfeld

pick your chances:    ?

What you all know already about risk …

threat ⊗ **vulnerability** ⊗ **impact**

likelihood

… and you will be left with residual risk
that you must be able to absorb …

https://www.dailycal.org/2017/06/30/14-things-kill-people-sharks/
http://www.tylervigen.com/spurious-correlations

sharks: ~10/a, flattened by TV: 41/a, coconuts: urban legend puts that at 150/a … well…. maybe just a handful … see https://en.wikipedia.org/wiki/Death_by_coconut

Protection and controls are a response to risk

date, and limiting access controls as much as possible. This document does not cover basic computer hygiene or system administration. This document is intended to cover the *other* 20% that basic hygiene and administration *do not* cover well.

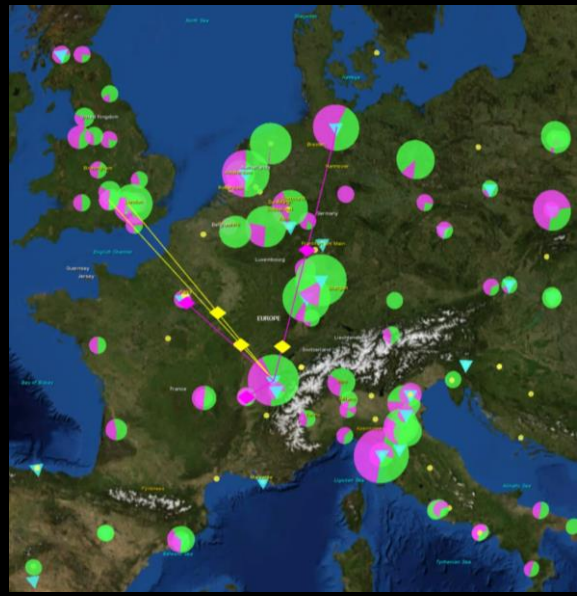
5. Bad Things Can Happen to Good Science

There are numerous examples of Open Science projects being affected by attacks over computer networks. Some of these attacks have specifically targeted the science projects, while in other examples, science projects have simply been collateral damage. Several real examples, with identifying details

Open Science Cyber Risk Profile, supported by TRUSTED CI THE NSF CYBERSECURITY CENTER OF EXCELLENCE, ESnet ENERGY SCIENCES NETWORK, National Science Foundation WHERE DISCOVERIES BEGIN

Peisert, Sean, Von Welch et al. *Open Science Cyber Risk Profile (OSCRP)*, March 2017, http://hdl.handle.net/2022/21259

All kinds of risk ..
… e.g. to our LHC Tier-1 global research collaboration



a big thank-you to Luca and his team at CNAF for the talk and sharing lessons learnt

CHEP2018 [EPJ Web of Conferences 214, 09008 (2019) https://doi.org/10.1051/epjconf/201921409008]

Your ICT systems as part of the global network

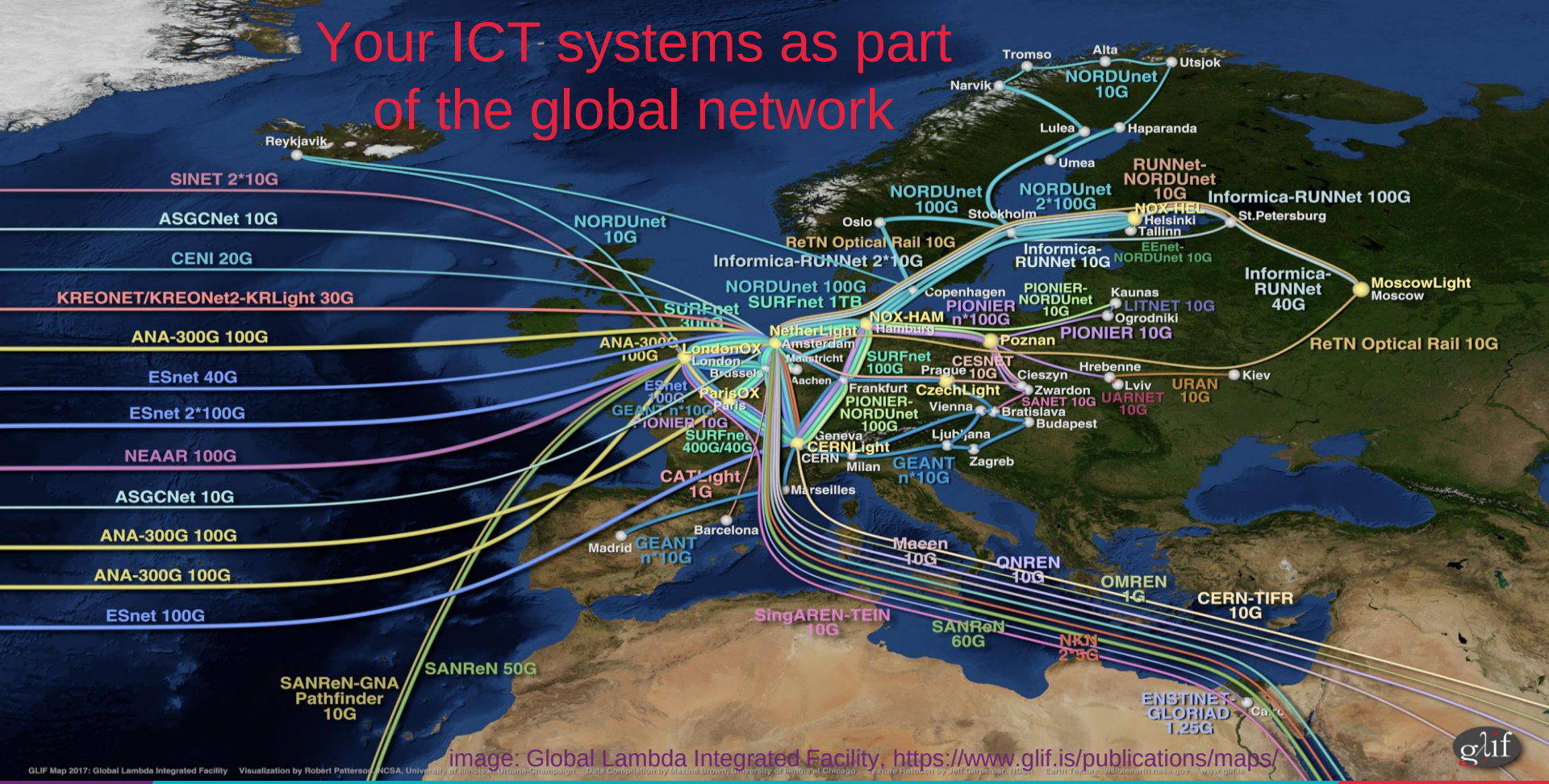


image: Global Lambda Integrated Facility, https://www.glif.is/publications/maps/

Our IT is just as connected as our researchers

Federated and research access for IT need not conflict with security

as long as you are aware of your risks, work together with your collaborations and peers,

and you can build *commensurate protection* for different classes of data and systems

Classifying the ‘Crown Jewels’ worth protecting

From data-centric viewpoint?

critical infrastructure information for recovery

research data
- irrecoverable
- processed

replicated community data

high risk information – safety and health

personal data
sensitive, ‘impactful’, …

Or from a resource and cost viewpoint?

using networks for personal use, youtube-dl, &c

finding a bitcoin miner in an isolated ‘on-prem’ cloud?

network abuse to call many, expensive phone numbers??

finding a bitcoin miner on HR desktop computers?????

In the end…

it is all about
'risk appetite'

- **protection**
  and commensurate response
- **detection**
- **response**
- **recovery**

Thanks to the folk at NorthWood LAN party 7 - http://www.linuxno.de/ - for staging this picture!

We the people …

- **CEO fraud and ‘whaling’**
- **system administrators and IT staff**
  … have lots of access rights and
  the need to use it often
- **researchers** that can (over)write unique data
- for physical access, **janitorial staff** are almost omnipotent

People are the weakest link in security of systems
… and the ‘most powerful person’ can … be anyone

Awareness

"Apparently, hackers really do still party like it's 1999," Verizon said in its 2015 Data Breach Investigations Report (DBIR) regarding how often really old vulnerabilities a

"common denominator—accounting for nearly 90% of all incidents—is people."

Oldies are still goodies as the Verizon team added:

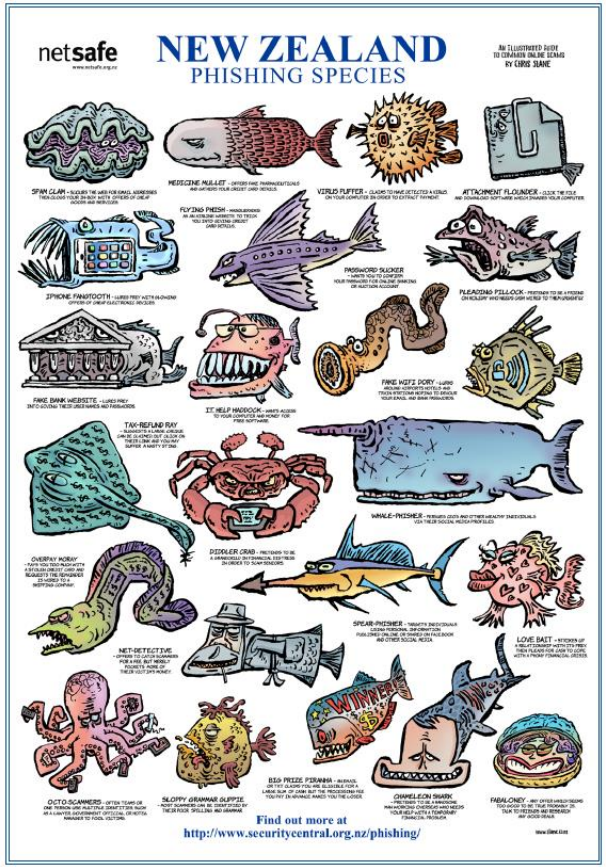
> Whether it's goofing up, getting infected, behaving badly, or losing stuff, most incidents fall in the PEBKAC and ID-10T über-patterns. At this point, take your index finger, place it on your chest, and repeat "I am the problem," as long as it takes to believe it. Good—the first step to recovery is admitting the problem.

When it comes to phishing attacks, the Verizon team found that 23% of users open phishing emails and 11% take the extra PEBKAC step of actually clicking on the attachment. Even a small phishing campaign of 10 emails has a 90% chance of

is a mere one minute and 22 seconds.

Don't forget to patch old vulnerabilities

According to the report, "99.9% of the exploited vulnerabilities had been compromised more than a year after the associated CVE was published." It's a

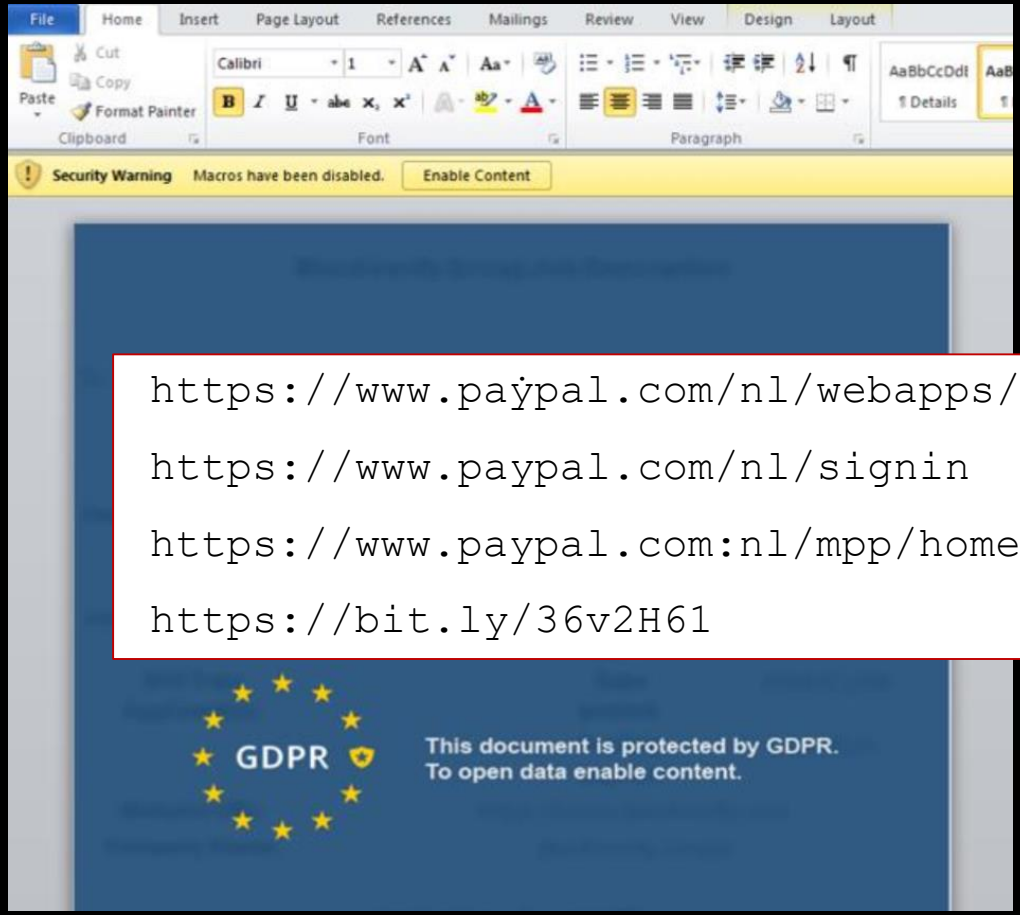


By Darlene Storm, Computerworld | 15 April 2015 16:47 CEST
https://www.computerworld.com/article/2910316/90-of-security-incidents-trace-back-to-pebkac-and-id10t-errors.html

Thanks to NetSAFE NZ
https://www.netsafe.org.nz/phishing/

Most Users Click …

… of gewoon Emotet malware email
(van het Epoch3 kartel deze week)



https://www.paypal.com/nl/webapps/mpp/account-selection

https://www.paypal.com/nl/signin

https://www.paypal.com:nl/mpp/home@my-account.info/view

https://bit.ly/36v2H61

FACTUUR J-192 van [naam]
Fact. 0680888 van [naam]
Fact. 2020-LIA20087 van [naam]
n [naam]
n [naam]
m]
naam]
van [naam]
am]
n [naam]
]
[naam]
Inv 40845 van [naam]
Schatting 13544 van [naam]
Schatting 152750-2020 van [naam]
Schatting 8135 van [naam]
Schatting PZB515-08.2020 van [naam]
Schatting h77468972-08.2020 van [naam]
Schatting v5588978-08.2020 van [naam]

https://labs.f-secure.com/assets/BlogFiles/f-secureLABS-tlp-white-lazarus-threat-intel-report2.pdf

Engaging users – that is: targets

Sources CERN (https://security.web.cern.ch/training/fr/posters.shtml)
UC System (https://security.ucop.edu/resources/security-awareness/phishing-2019-campaign.html) and Yale University (Patrick Lynch)

From Nikhef CSIRT <security@nikhef.nl> Reply Forward Redirect Archive Junk Delete More

Subject **Login of David X Groep (xdavidg) to Nikhef from an unusual location: Amsterdam, Nether...** 1:06

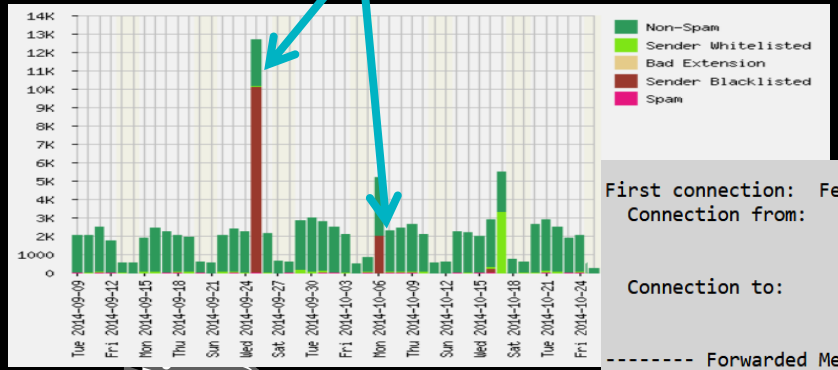
To xdavidg@nikhef.nl

```
[English follows Dutch]

Geachte David X Groep,

U, of iemand die zich als u voordeed, heeft ingelogged vanaf onderstaande
locatie. U ontvangt deze waarschuwing omdat het de eerste keer is dat u vanaf
deze plek inlogde. Wilt u controleren of u het inderdaad zelf was die
hiervandaan inlogde? En zo niet, ons - de Nikhef helpdesk op telefoonnr 2200,
zie onder - onmiddellijk waarschuwen?

  Eerste verbinding op: Aug 13 20:54:32
  Verbinding vanaf:     XS4ALL XS4ALL Internet BV
                        Amsterdam, Netherlands (of omgeving)
                        82.[redacted] ([redacted]xs4all.nl)
  Gebruikte dienst:     Email reading (with an IMAP client)

Is de verbinding inderdaad door u gemaakt?

- als dat NIET ZO IS:
  dan is er op uw account xdavidg@nikhef.nl waarschijnlijk ingebroken.
  Neem direct contact op met de Nikhef helpdesk, op telefoonnummer
  020 592 2200, of stuur een mail naar security@nikhef.nl

- was u dit WEL:
  u kunt deze mail negeren. U krijgt dan geen verdere meldingen
```

Segmentation of access rights

Through phishing, outsiders and attackers will appear as insiders
… so limit what insiders can do to what's needed
… but don't go overboard with your IGA

compromised accounts @Nikhef
(abuse contained with SURFmailfilter)




```
First connection:  Feb 15 07:19:41
  Connection from:   Subnet Nos Oignons chez TTNN Route for Tetaneutral.net 157/24
                     Goyrans, France (or nearby)
                     89.234.157.254 (marylou.nos-oignons.net)
  Connection to:     Email reading


-------- Forwarded Message --------
Subject: Login of [redacted] ([redacted]) to Nikhef from an unusual
 location: Goyrans, France
Date:   Wed, 15 Feb 2017 07:01:45 +0000
From:   Nikhef CSIRT <security@nikhef.nl>
```

Although sometimes …

```
LO0.AR5.ENSCHEDE1.SURF.NET 3613:
  NOV 20 07:20:50.927 UTC: %ENV_MON-2-TEMP:
  +HOTPOINT TEMP SENSOR(SLOT 18) TEMPERATURE HAS
REACHED WARNING LEVEL AT 61(C)
FEW SECONDS LATER ON THE LOCAL SIDE:
LO0.CR2.AMSTERDAM2.SURF.NET 1146:
  NOV 20 07:20:56.458 UTC: %CLNS-5-ADJCHANGE: +ISIS:
  ADJACENCY TO AR5.ENSCHEDE1 (POS2/0) DOWN, INTERFACE
DELETED(NON-IIH)
```

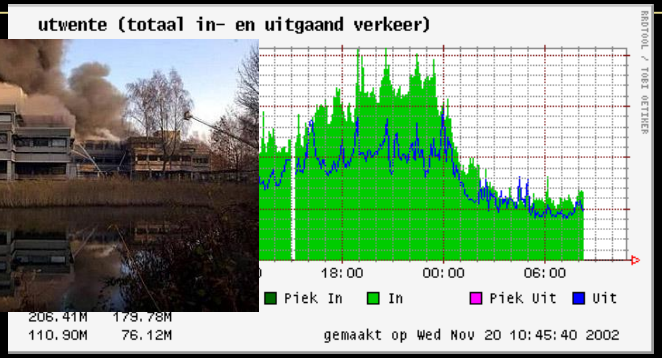
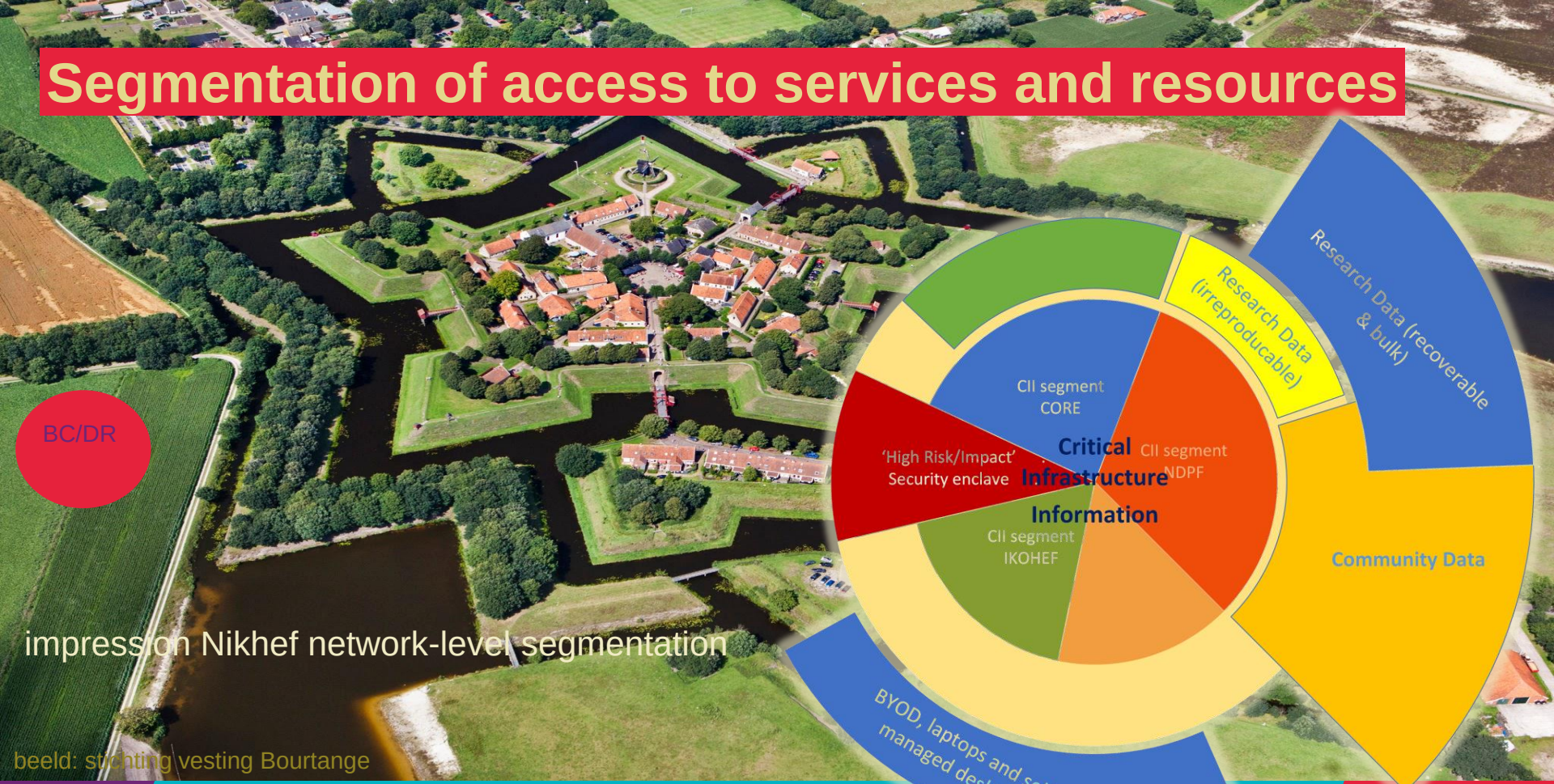


Image: PS control room at CERN

See also http://www.independent.co.uk/news/marital-row-blows-fuse-on-big-bang-theory-1573588.html

Segmentation of access to services and resources



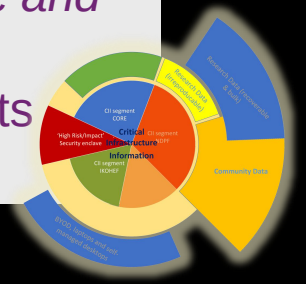
impression Nikhef network-level segmentation

beeld: stichting vesting Bourtange

Segmentation: a research network with office enclaves

… you want a **science network**
with a ‘back-office enclave’

‘open-core’ research network model implements enclave structure *and* protects against overload by having no stateful components in the network path

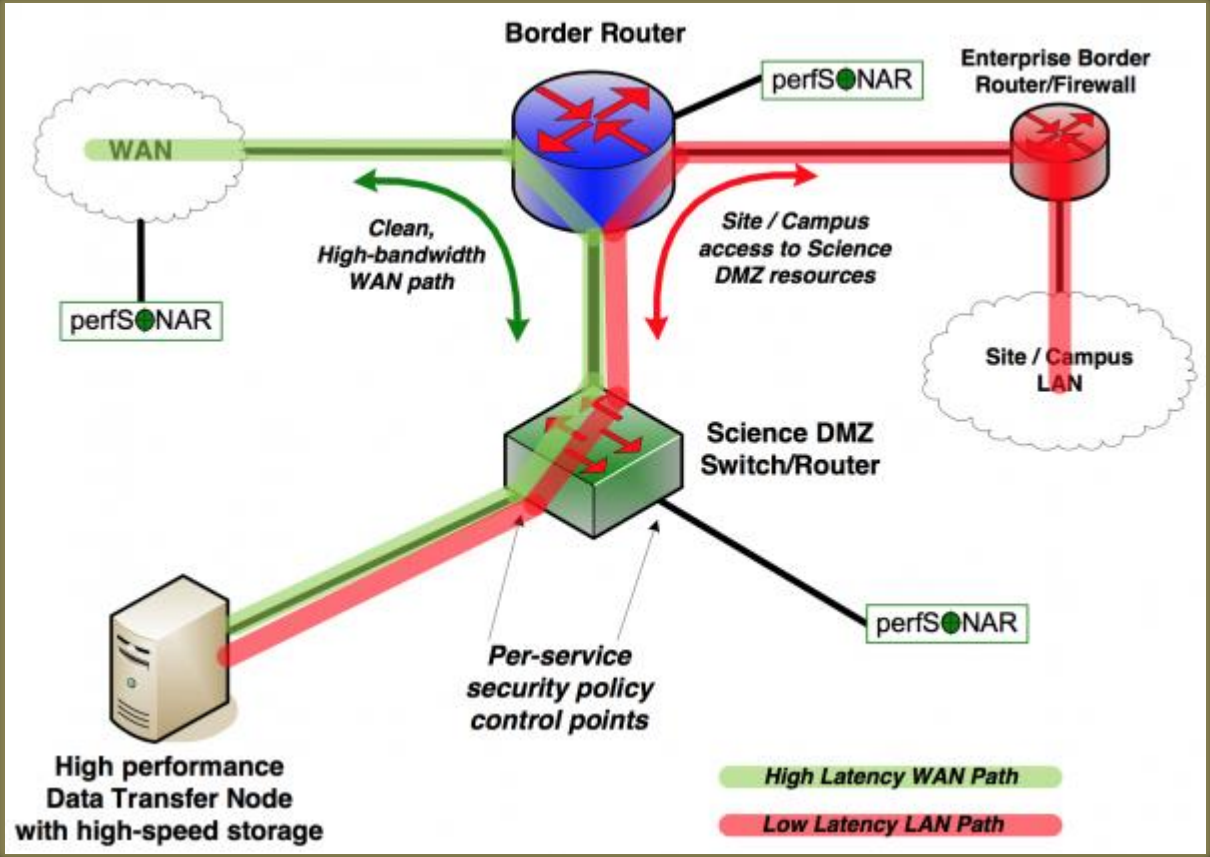


network just one of a series of controls,
alongside host-based controls, service-level controls, and object-identity-level controls
the open-core model implements the enclave structure *and* allows open research federation

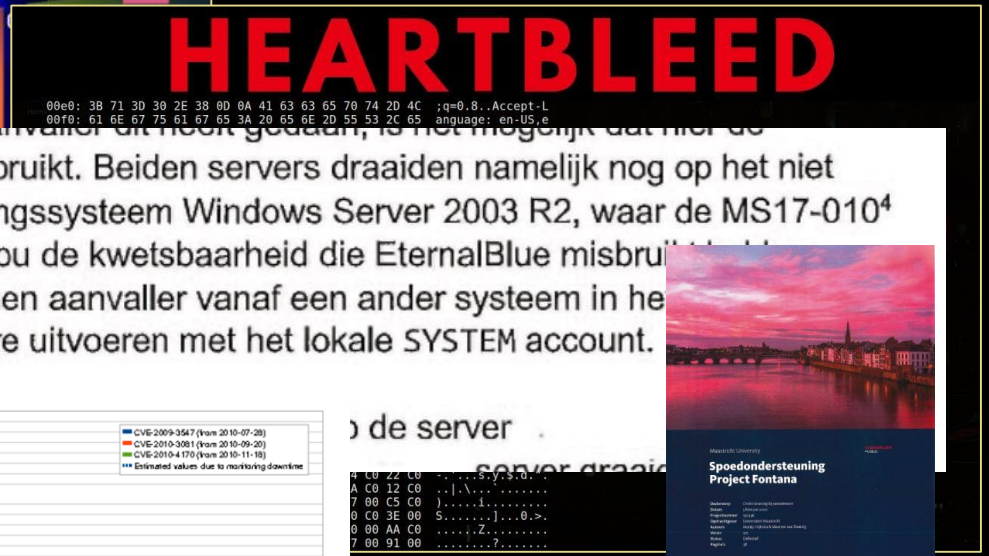
‘ScienceDMZ’

Network protection does mean cutting it off from the outside

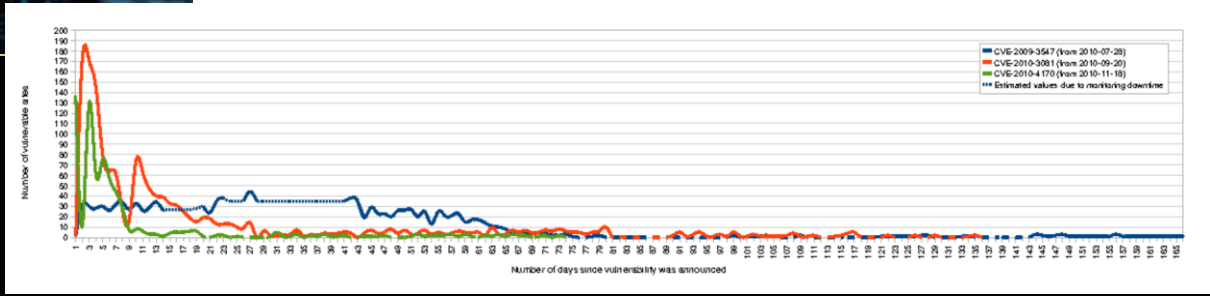
remember that first presentation in the UM symposium …



Once the attacker is in – he lies in waiting …



zogenaamde EternalBlue exploit voor is gebruikt. Beiden servers draaiden namelijk nog op het niet langer door Microsoft ondersteunde besturingssysteem Windows Server 2003 R2, waar de MS17-010[4] patch niet op is geïnstalleerd. Deze patch zou de kwetsbaarheid die EternalBlue misbruikt verholpen. Met de EternalBlue exploit kan een aanvaller vanaf een ander systeem in het toegang krijgen tot doel-systeem en malware uitvoeren met het lokale SYSTEM account.



CVE-2020-1350, July 14th, 2020

https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin:-exploiting-a-17-year-old-bug-in-windows-dns-servers/

Response … it’s always a balance …

security is a balance of risk, usability, and cost

Response capabilities – team work

‘Strategic’ level

do you want to react & prevent reoccurrence?

report to LE, or recover services?

if you suddenly find yourself in the news?

trust and delegation for operational response?

‘Operational’ level – your Computer Security Incident Response Team (CSIRT)

“if there's something weird, and it don't look good – who you gonna call?”

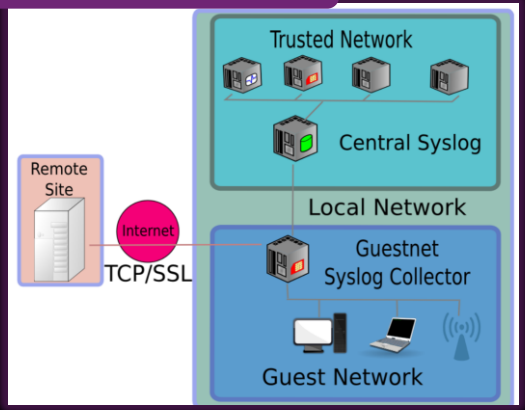
detecting something is weird in the first place

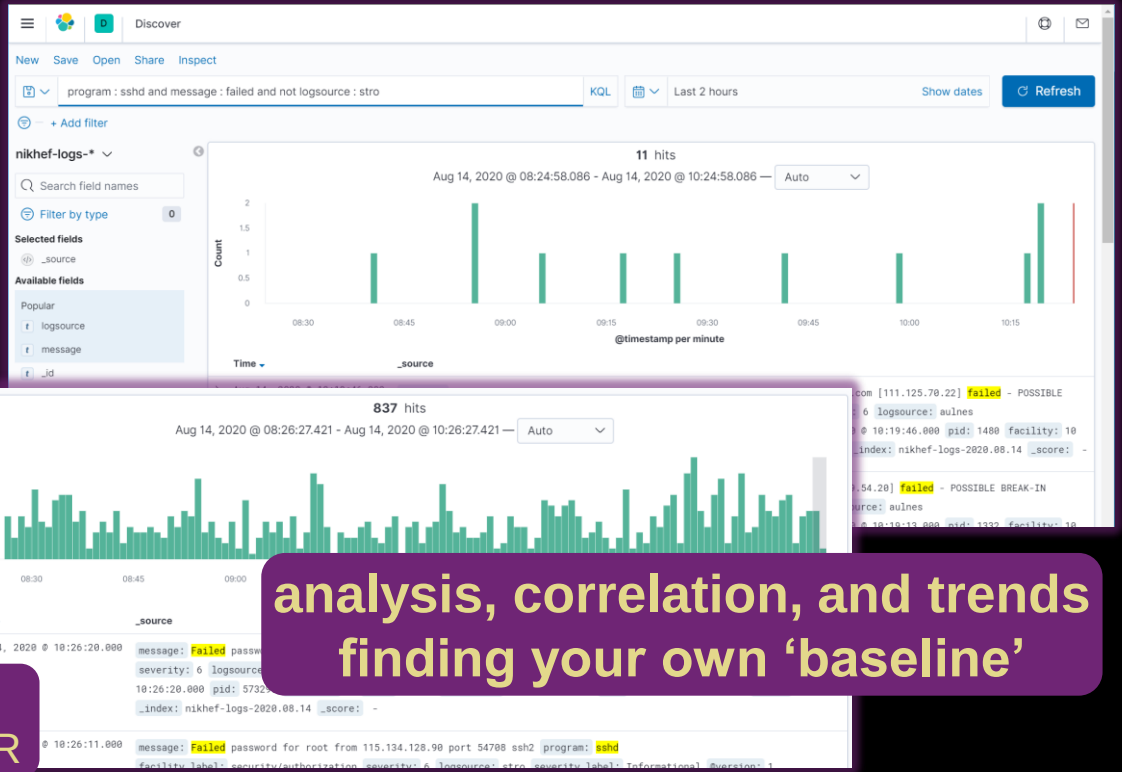
An attacker! …
… or maybe a PhD student?

“a pint of sweat will save a gallon of blood”

You *will* be had – but how, and when, do you know?

collection of data





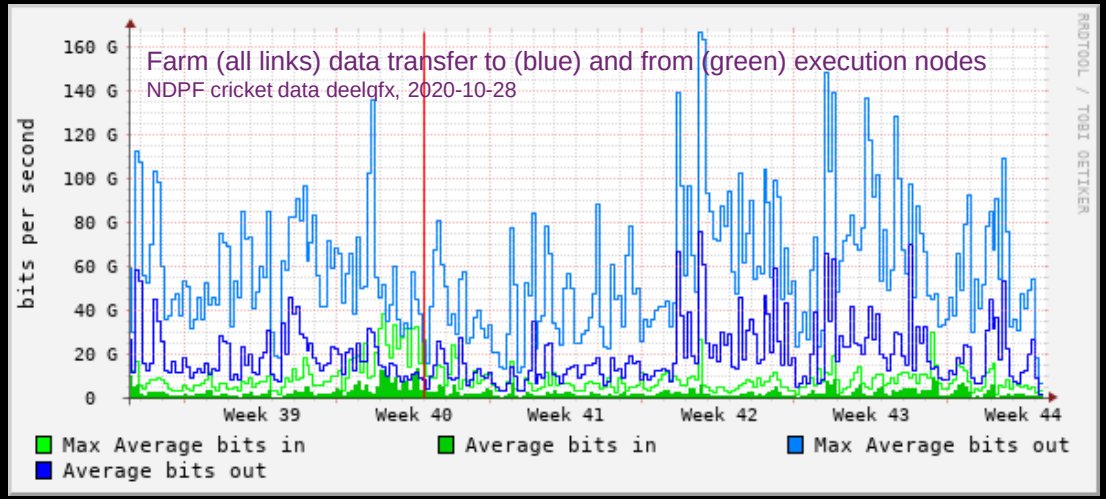
analysis, correlation, and trends
finding your own ‘baseline’

also helps determine specific scope and impact of data breaches for GDPR

On COTS ‘commercial’ IDS firewalls and SOC offerings

Commercial providers take care of some of the intel gathering for you but they do that for their ‘average’ customer, and will not see community, or research, specific threats or patterns

- many false positives likely
  our standard research traffic to ‘the enterprise world’ looks like an attack: DoS, DDoS, unusual traffic, connections from all over the world
- COTS SOCs of limited value
  for a research IT infrastructure (but may be perfectly good match for student dorms and within specific ‘enterprise enclaves’)



The marketing spiel: ‘we block 3000 attacks per hour!’

Discover

New Save Open Share Inspect

program: sshd and message: "failed password for" and not message: git and not logsource: hekel | KQL | Last 12 hours | Show dates | Refresh

+ Add filter

nikhef-logs-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

Popular

t _id

_score

t logsource

Top 5 values in 500 / 500 records

fiora 39.2%

stro 34.4%

solnan 19.2%

lena 7.2%

t message

t program

t _index

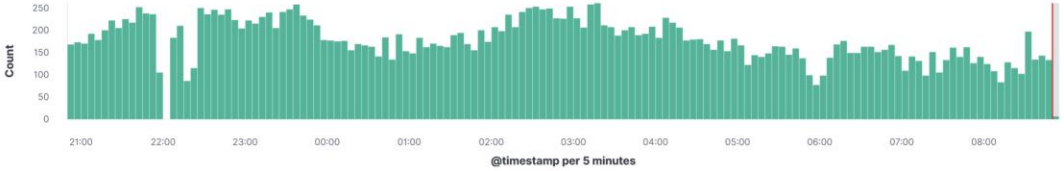
t _type

@timestamp

t @version

25,682 hits

Aug 24, 2020 @ 20:50:28.253 - Aug 25, 2020 @ 08:50:28.253 — Minute Scaled to 5 minutes



Time	_source
Aug 25, 2020 @ 08:50:24.000	program: sshd message: Failed password for root from 222.186.42.57 port 43436 ssh2 priority: 86 @version: 1 severity: 6 facility_label: security/authorization severity_label: Informational facility: 10 timestamp: Aug 25 08:50:24 pid: 481993 @timestamp: Aug 25, 2020 @ 08:50:24.000 type: syslog logsource: stro _id: 455hJHQBEOkKLjoh0hpS _type: _doc _index: nikhef-logs-2020.08.25 _score: -
Aug 25, 2020 @ 08:50:17.000	program: sshd message: Failed password for root from 222.186.42.57 port 43436 ssh2 priority: 86 @version: 1 severity: 6 facility_label: security/authorization severity_label: Informational facility: 10 timestamp: Aug 25 08:50:17 pid: 481993 @timestamp: Aug 25, 2020 @ 08:50:17.000 type: syslog logsource: stro _id: fChhJHQBBg1VRchytu_U _type: _doc _index: nikhef-logs-2020.08.25 _score: -
Aug 25, 2020 @ 08:50:11.000	program: sshd message: Failed password for invalid user html from 211.197.28.252 port 60442 ssh2 priority: 86 @version: 1 severity: 6 facility_label: security/authorization severity_label: Informational facility: 10 timestamp: Aug 25 08:50:11 pid: 481977 @timestamp: Aug 25, 2020 @ 08:50:11.000 type: syslog logsource: stro _id: Cp5hJHQBEOkKLjohogYr _type: _doc _index: nikhef-logs-2020.08.25 _score: -
Aug 25, 2020 @ 08:50:08.000	program: sshd message: Failed password for root from 222.186.42.57 port 15571 ssh2 priority: 86 @version: 1 severity: 6

Although DDoS *is* a very real risk

We *are* being targeted for extortion … although profitability is pretty low …

November saw an uptake of DDoS extortion against NRENs and other academic targets

and you have to work with upstreams and peers

the 'SURF wasmachine'

https://team-cymru.com/community-services/utrs/

https://www.geant.org/Services/Trust_identity_and_security/Pages/DDoS.aspx

https://events.geant.org/event/296/

so: reach out!

and implement BCP38 yourself to save the world

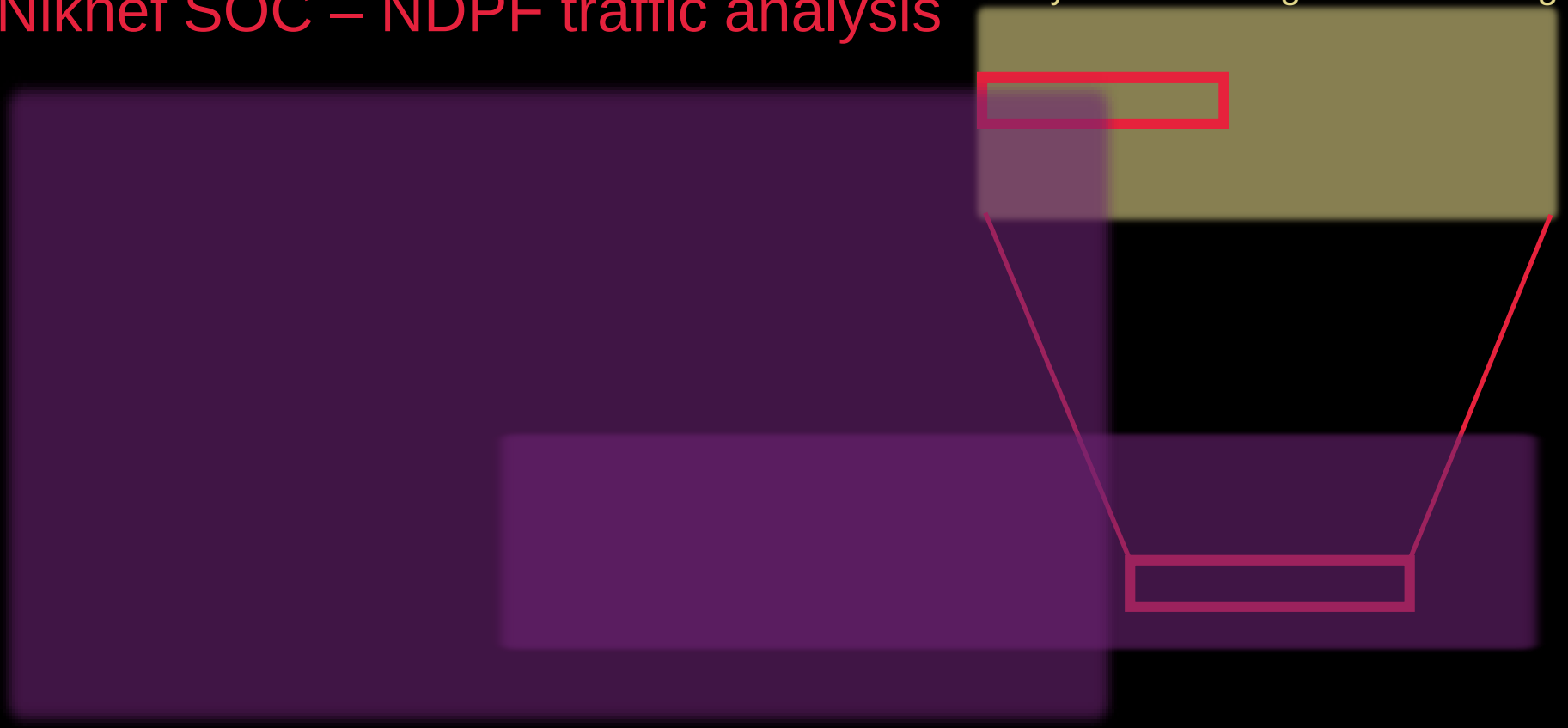
https://www.netscout.com/blog/asert/lazarus-bear-armada-lba-ddos-extortion-attack-campaign-october

https://blogs.akamai.com/sitr/2020/08/ransom-demands-return-new-ddos-extortion-threats-from-old-actors-targeting-finance-and-retail.html

https://www.senki.org/operators-security-toolkit/ddos-extortionist-behaviors/

Nikhef SOC – NDPF traffic analysis

many ‘false warnings’: needs tuning



NikhefSOC/NDPF ELK setup: Jouke Roorda

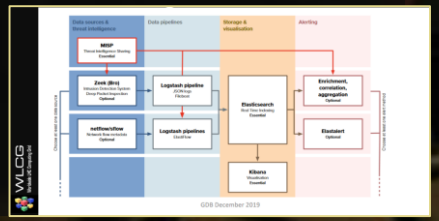
WLCG SOC WG

WLCG SOC concept targeted at data intensive research

combine those elements of monitoring and capabilities
that match usage pattern and scale to desired flow rate
a COTS/commercial SOCs will say all of our traffic is a DoS ☺

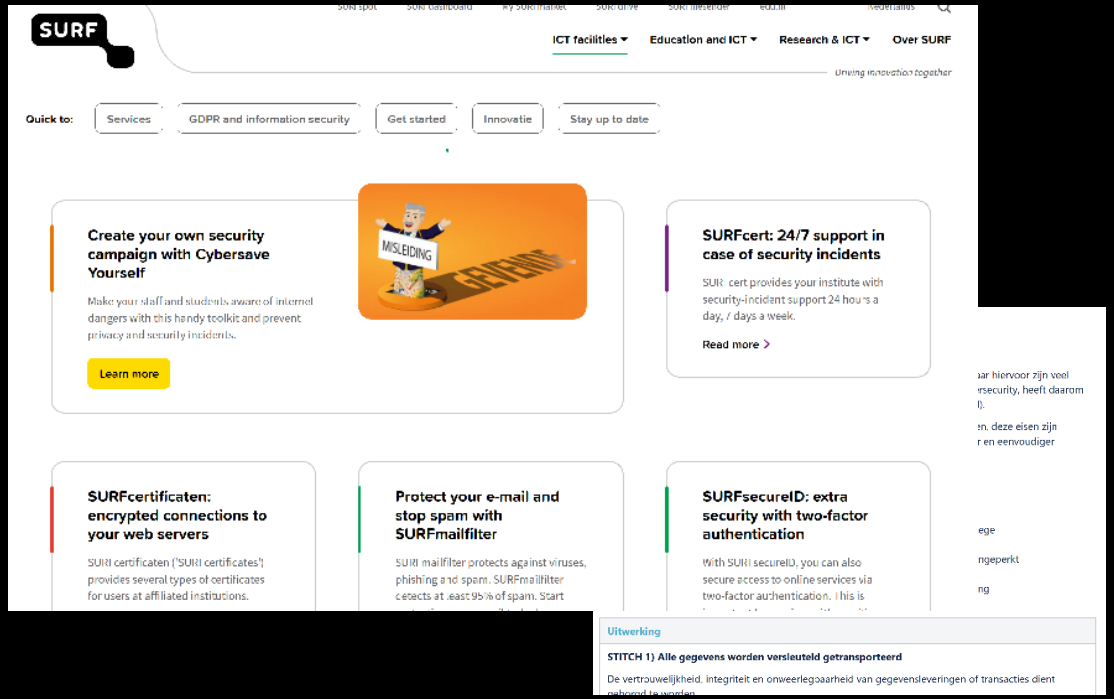
Leverage our community – our unique feature!
MISP sharing of IoCs, trusted sources, and … contribute back

Zeek mirrored-monitoring of known IoCs
*since all we do **must** be stateless*



Sharing intelligence between organisations

through the Dutch SURF constituency & its trainings



… and beyond

TF-CSIRT Trusted Introducer

FIRST Improving Security Together

APCERT Asia Pacific Computer Emergency Response Team

EGI CSIRT

lacnic warp Warning Advice and Reporting Point

REN-ISAC

AfricaCERT United in promoting cyber security in Africa

in international security forums and trust groups

Trust groups

Beyond ‘organisational’ trust - contribute and participate …
… and you will reap the benefits in turn

Participation is critical to making this work
You need your OpSec people to ‘get around’, meet, and work, globally
starting with TRANSITS-I nationally is a good initiation

at a GEANT TRANSITS-I training @ APAN 2019, MY

Trust, sharing, and sharing back …

yet trust does not scale well - without ‘process’ – beyond Dunbar’s Number

so for the more relevant and valuable trust groups, there are processes

But what to do with all this ? … and Cit0day is just one …

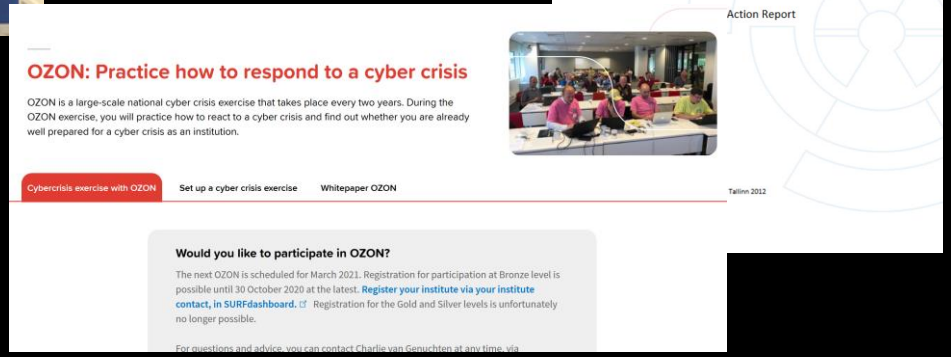
sharing responsibly in bulk fashion is hard without a CSIRT contact

… although some of you may have gotten this last week via our eduGAIN, EGI & CERN effort

… and moreover the data is really old

although sometimes you don’t need a password dump to get in, I think …

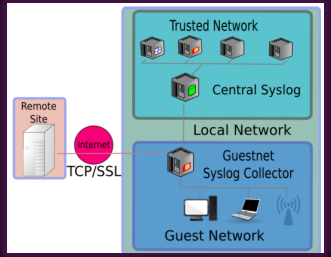
Exercise! From technical, to federated, to strategic



Assets: you may never know all – discover and exercise

Open collaboration and research: users are everywhere, and almost all are ‘BYOD’ … and creative enough to find any loophole (which is actually a Good Thing™ …)

Asset modelling should support flexibility without loosing containment and response, using monitoring



Nikhef

Nikhef CSIRT Traceability Challenge

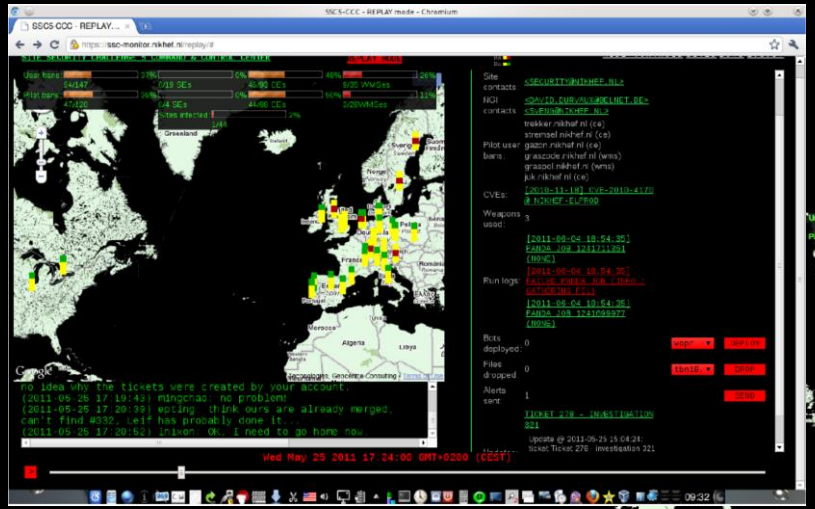
Introduction

Deze Traceability Challenge bestaat uit drie onderdelen, in (naar verwachting) oplopende moeilijkheidsgraad. Iedere challenge begint met een externe ‘trigger’ – aan het eind van dit document staan de hints en de goede (of in ieder geval: de ‘gewenste’) oplossing.

Veel plezier!

Know your users and what you can expect as ‘typical behaviour’ – this means personal knowledge *and then exercise to see if you indeed act*

… the joy of testing – simulated incidents



Communication:

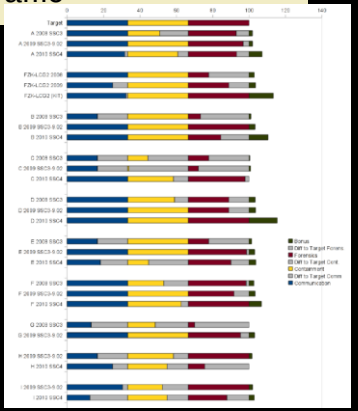
- Endpoints valid?
- Form/Content OK ?

Containment

- Ban "malicious" users
- Find/Stop malicious processes
- Find submission IP

Forensics

- Basic Forensics on binary
- Network traffic



News is unpredictable … more about framing than reality

in reality, this was the (admittedly unsecured) console of a cloud analysis VM in the UK, loading some read-only software of the LHCb experiment, not allowing interactive login anyway!

And what you don’t want … the Uni-Gießen way

source: www.krone.at

source: www.hessenschau.de

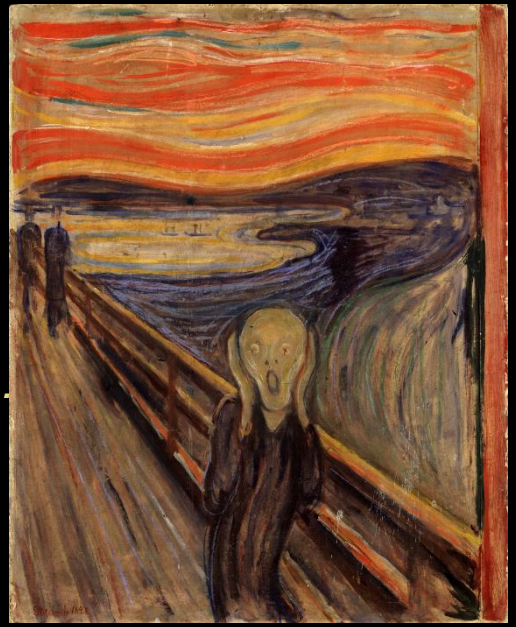
You hear that you're compromised … and now what?

1. Have a coffee! .. and then think first …
   the intruder has typically been there
   for 3-6 months already …

2. Who do you call? Who can you call?
   Engage your operational security team!
   and if you, or they, get stuck, there is a community
   that can help you, including SURFcert and peers …

3. Priorities: limit damage, but do not destroy evidence

4. Activate your BC/DR plan and resources if needed



Recommendations … *as delivered to your management*

- **Do get all people engaged** in the institute and create awareness, and allow for effort in IT service management – but IT security is more than just the IT team
- **Do maintain an operational response capability**, or develop it if you don't have one already – and integrate it with the national and global community – they have to 'get around' to be effective and engender trust in the community
- **Don't be afraid** of bad things – they will happen anyway. Challenge is to know your risks, reduce unnecessary risks, and be able to absorb the rest –containment, resilience, and recovery capabilities are the key *(and they will help determine and limit the impact of data breaches as well)*
- **Don't loose sight of the mission** and goals of the institute – our high-level aim

“Доверяй, но проверяй”

Russian proverb – “trust, but verify”

Nikhef

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

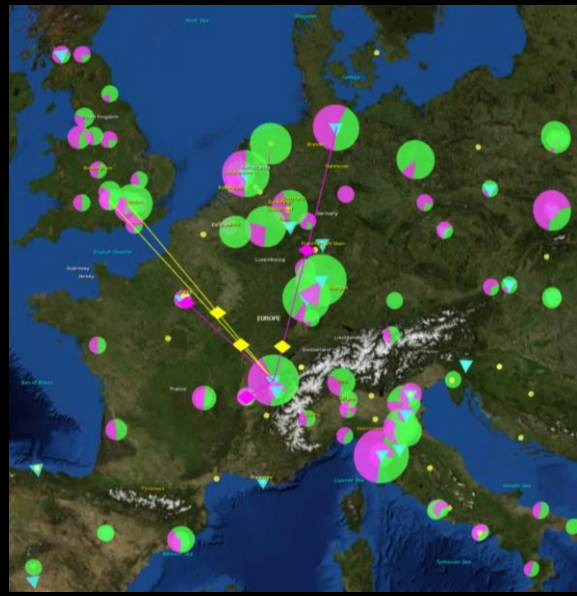
BC/DR planning

BC/DR can be at several levels – and doing it really well is very, very expensive
esp. the testing part, since if you *do* cover all aspects and you're not Tier-4 for both infra and services, it will be 'invasive and 'visible' to end-users

But BC/DR planning is important, and some things around esp. communications can be prepared well

- make sure there are alternative (maybe luke-warm?) (web) communications ready to go
- make sure these are actually fully independent: no shared single upstream network, different geographical location, different power (sub)stations, distinct user/admin credentials, independent systems management … but still keep patching it of course ☺
- backup for local access: different out-of-band uplink, either over 4G or a different upstream ISP … and over a different router!
- make sure that key personnel knows how to use it

All kinds of risk .. business Continuity/Disaster Recovery – e.g. in our (redundant) LHC Tier-1 global network



CHEP2018 [EPJ Web of Conferences 214, 09008 (2019) https://doi.org/10.1051/epjconf/201921409008]

But if your payroll processing data centre looks like this …

you may need slightly more investment in BC/DR –
and Northgate Plc. indeed did & managed to pay on time

imagery: HSE, https://www.hse.gov.uk/comah/buncefield/

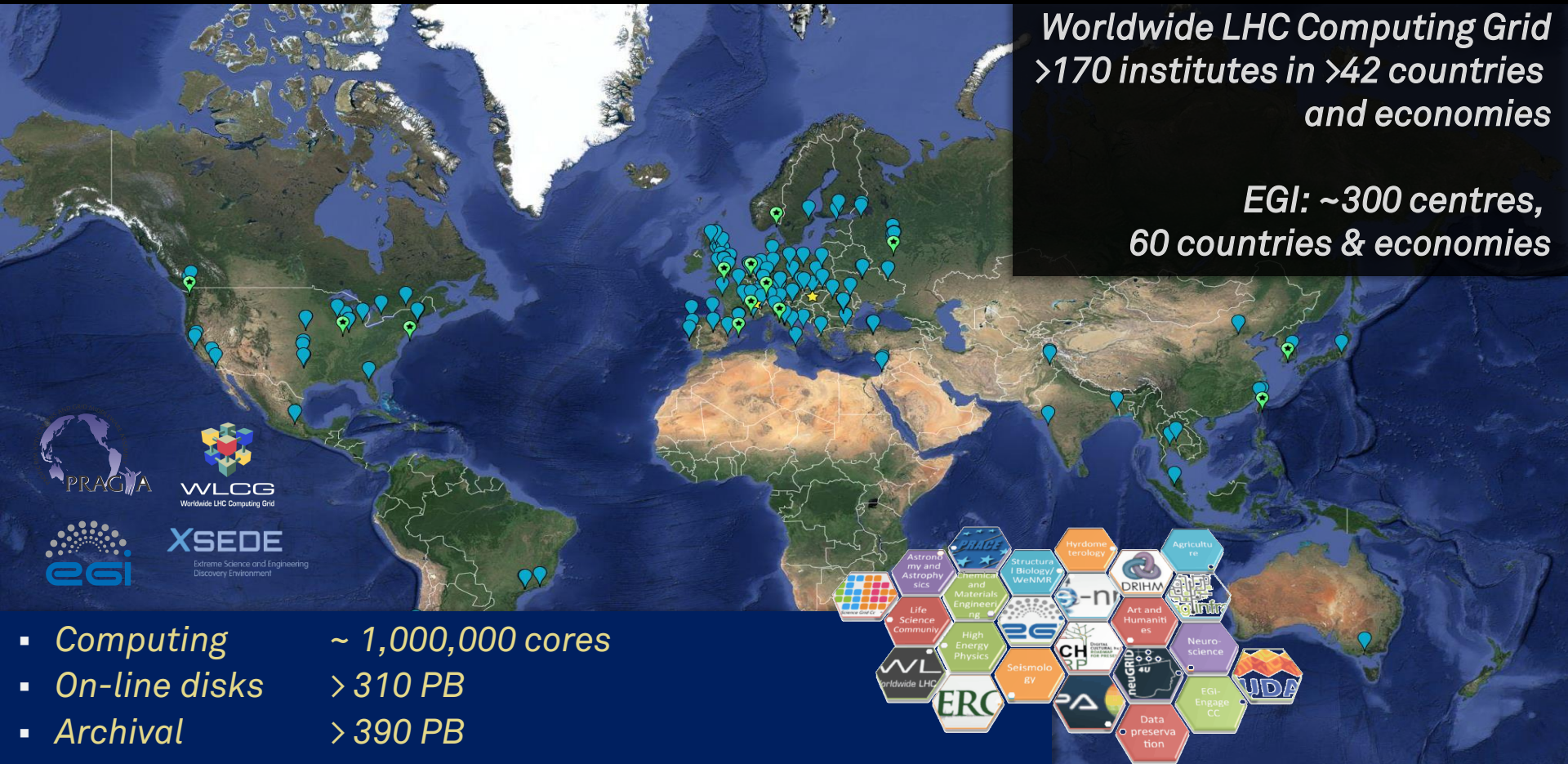
Evoswitch (IronMountain) mini-BC/DR location Nikhef

- communications infra
- recovery information
- stand-by for global services, like e-Infra authn websites, trust anchors
- ability to host red-team services (duringexercises ☺)

At least you get

- independent geography (not same watersystem, even if HHNK), separate power plant and substations, different fibre routes, independent AS and IP space, separate security and guard systems
- and still full access for designated staff

The Importance of Being Open – in Europe and beyond



Worldwide LHC Computing Grid
>170 institutes in >42 countries and economies

EGI: ~300 centres, 60 countries & economies

- *Computing* *~ 1,000,000 cores*
- *On-line disks* *> 310 PB*
- *Archival* *> 390 PB*

Beyond a single organisation

‘Enterprise standards’ and classifications can only be inspirational, not used as-is!


National Institute for Subatomic Physics

Nikhef

CONFIDENTIAL

Nikhef NDPF IT standard technical and organisational measures

Introduction and scope

The Nikhef NDPF IT standard technical and organisational measures (TOM) for IT services apply to those services and systems ("in-scope Services") that are part of the Nikhef Data Processing Facility (NDPF), designated to provide services to the Target Audience, and are not otherwise covered by more specific TOM documents.

The Target Audience for in-scope services is defined to be Nikhef employees and registered guests, authorised visitors, users of the NDPF Services in the scope of the Dutch National e-Infrastructure coordinated by SURF, and partners in federated infrastructures in which Nikhef participates and that have been designated as an in-scope target audience by explicit designation or by default.

In-scope Services are those services that are managed and operated by or provided under the authority of the Computer Technology (CT) group and/or the Physics Data Processing (PDP) programme that are in addition intended to be used by the Target Audience ("managed services").

Contents


WISE COMMUNITY

A Trust Framework for Security Collaboration among Infrastructures

SCI version 2.0, 31 May 2017

L Florio[1], S Gabriel[2], F Gagadis[3], D Groep[2], W de Jong[4], U Kaila[5], D Kelsey[6], A Moens[7], I Neilson[6], R Niederberger[8], R Quick[9], W Raquel[10], V Ribaillier[11], M Sallé[2], A Scicchitano[12], H Short[13], A Slagell[14], U Stevanovic[14], G Venekamp[2] and R Wartel[13]

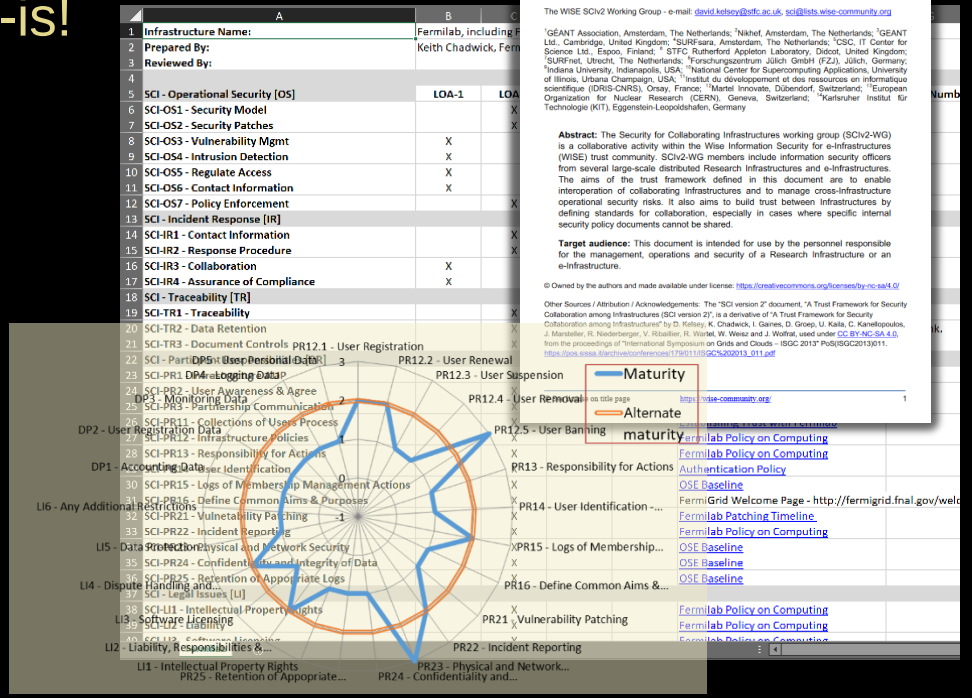
The WISE SCIv2 Working Group - e-mail: david.kelsey@stfc.ac.uk, sci@lists.wise-community.org

[1]GÉANT Association, Amsterdam, The Netherlands; [2]Nikhef, Amsterdam, The Netherlands; [3]GÉANT Ltd., Cambridge, United Kingdom; [4]SURFsara, Amsterdam, The Netherlands; [5]CSC, IT Center for Science Ltd., Espoo, Finland; [6] STFC, Rutherford Appleton Laboratory, Didcot, United Kingdom; [7]SURFnet, Utrecht, The Netherlands; [8]Forschungszentrum Jülich GmbH (FZJ), Jülich, Germany; [9]Indiana University, Indianapolis, USA; [10]National Center for Supercomputing Applications, University of Illinois, Urbana Champaign, USA; [11]Institut du développement et des ressources en informatique scientifique (IDRIS-CNRS), Orsay, France; [12]Martel Innovate, Dübendorf, Switzerland; [13]European Organization for Nuclear Research (CERN), Geneva, Switzerland; [14]Karlsruher Institut für Technologie (KIT), Eggenstein-Leopoldshafen, Germany

Abstract: The Security for Collaborating Infrastructures working group (SCIv2-WG) is a collaborative activity within the Wise Information Security for e-Infrastructures (WISE) trust community. SCIv2-WG members include information security officers from several large-scale distributed Research Infrastructures and e-Infrastructures. The aims of the trust framework defined in this document are to enable interoperation of collaborating Infrastructures and to manage cross-Infrastructure operational security risks. It also aims to build trust between Infrastructures by defining standards for collaboration, especially in cases where specific internal security policy documents cannot be shared.

Target audience: This document is intended for use by the personnel responsible for the management, operations and security of a Research Infrastructure or an e-Infrastructure.

Other Sources / Attribution / Acknowledgements: The "SCI version 2" document, "A Trust Framework for Security Collaboration among Infrastructures (SCI version 2)", is a derivative of "A Trust Framework for Security Collaboration among Infrastructures" by D. Kelsey, K. Chadwick, I. Gaines, D. Groep, U. Kaila, C. Kanellopoulos, J. Marsteller, R. Niederberger, V. Ribaillier, R. Wartel, W. Weisz and J. Wolfrat, used under CC BY-NC-SA 4.0, from the proceedings of "International Symposium on Grids and Clouds – ISGC 2013" PoS(ISGC2013)011. https://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf



e.g. ISO27001 can help structure
or identify gaps in your knowledge,
but ISO27002 should not be blindly applied
without *your own* risk assessment and intelligence

Nikhef

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

Thanks to, with contributions of, material & ideas from, or discussion with …

Universiteit Maastricht, EGI CSIRT, GEANT TRANSITS, TF-CSIRT, AARC Community, Andrew Cormack, SIM3, KPK, Dave Kelsey, Hannah Short, Sven Gabriel, Luca dell'Angelo & INFN CNAF, Romain Wartel, CERN, Jouke Roorda, SURF & SURFcert, Alf Moens, Charlie van Genuchten, OZON & CLAW, Urpo Kaila, NetSAFE NZ, FoxIT, F-secure, NCSC-NL, FBI, Tristan Suerink, SURF SCIRT, Vienna TIIME meetings and unconference, KPMG (AT, NL), ISGC SecWS Taipei, Interoperable Global Trust Federation IGTF, David Crooks & Liviu Valsan & WLCG SOC WG, STFC RAL, TrustedCI & CTCS, WISE Community, CESNET, Daniel Kouřil
and lots of good stuff from groups and people preferring not to be named

but all views are of course my own and not necessarily shared by any of them …

background images from Unsplash: TCD library: @jzamora, cleaner: @verneho, sitting on a balcony: @nate_Dumlao, flood: @kellysikkema
Cyberdefense exercise room: Red Flag 17 (US DoD)
Edvard Munch "The Scream": painting now in Nasjonalgalleriet Oslo, UK crown jewels from WikiMedia Commons (public domain photo from 1952)