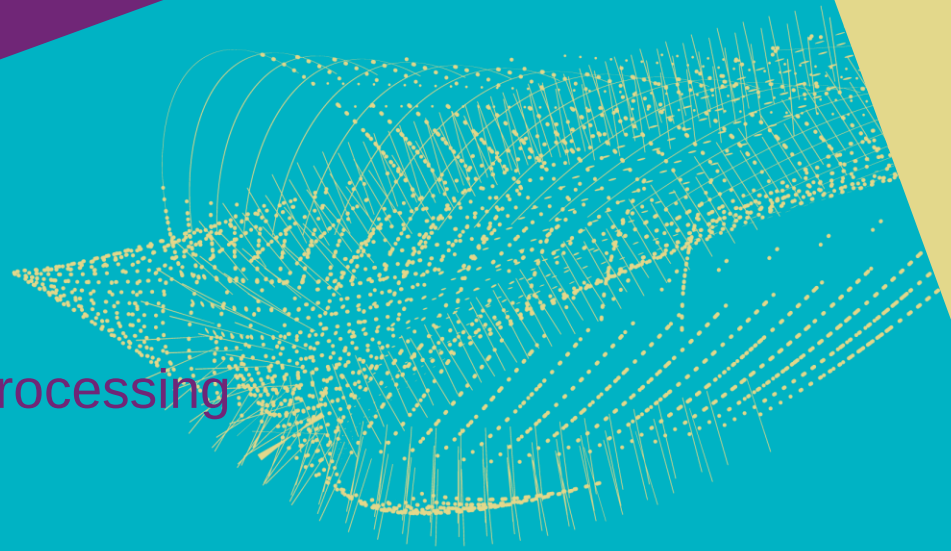
Nikhef



David Groep, Physics Data Processing

Staying reasonably safe in an open research environment

August 2020

Did anyone attend - or watch - the UM symposium?

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

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

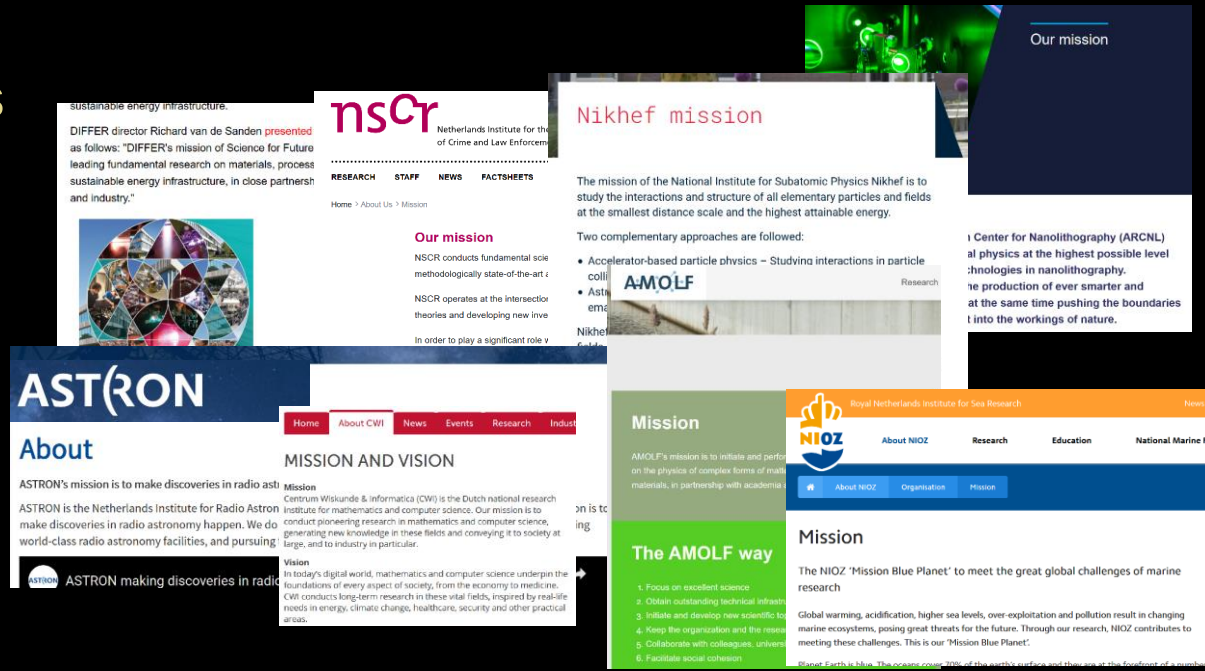
There are numerous examples of Open Science projects being affected by attacks over computer networks. Some of these attacks have specifically targeted the science projects, while in other examples, science projects have simply been collateral damage. Several real examples, with identifying details

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

A risk to *what*, exactly?

- to our research missions
- to our people & material and immaterial assets *systems, servers, data, archives, reputation,…*
- to science and society



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 …

pick your chances:    ?

Your ICT systems as part of the global network

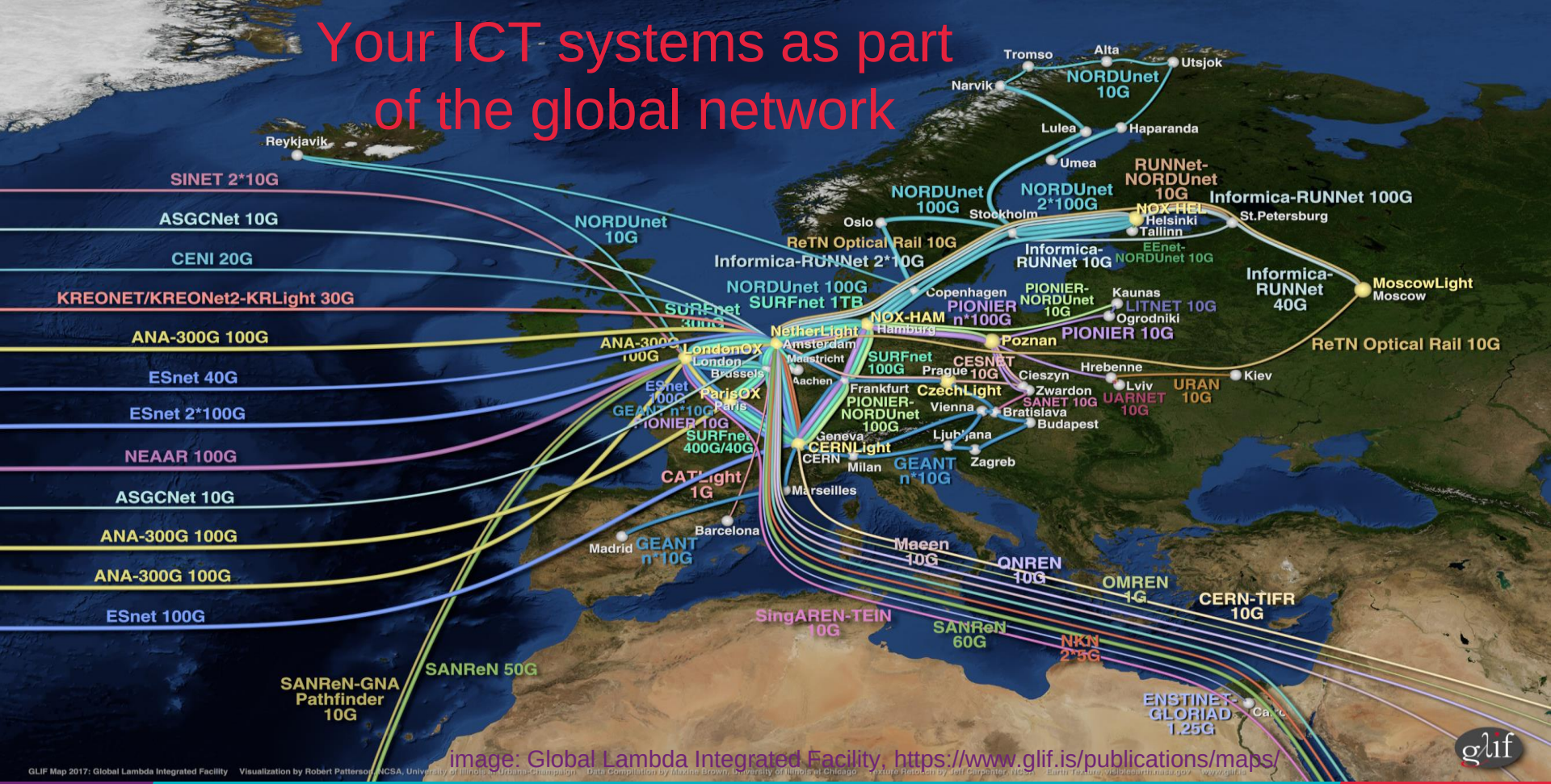


image: Global Lambda Integrated Facility, https://www.glif.is/publications/maps/

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

high risk information – safety and people

personal data: sensitive, impactful, …

research data

irrecoverable | processed

replicated community data

Or from a resource and cost viewpoint?

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

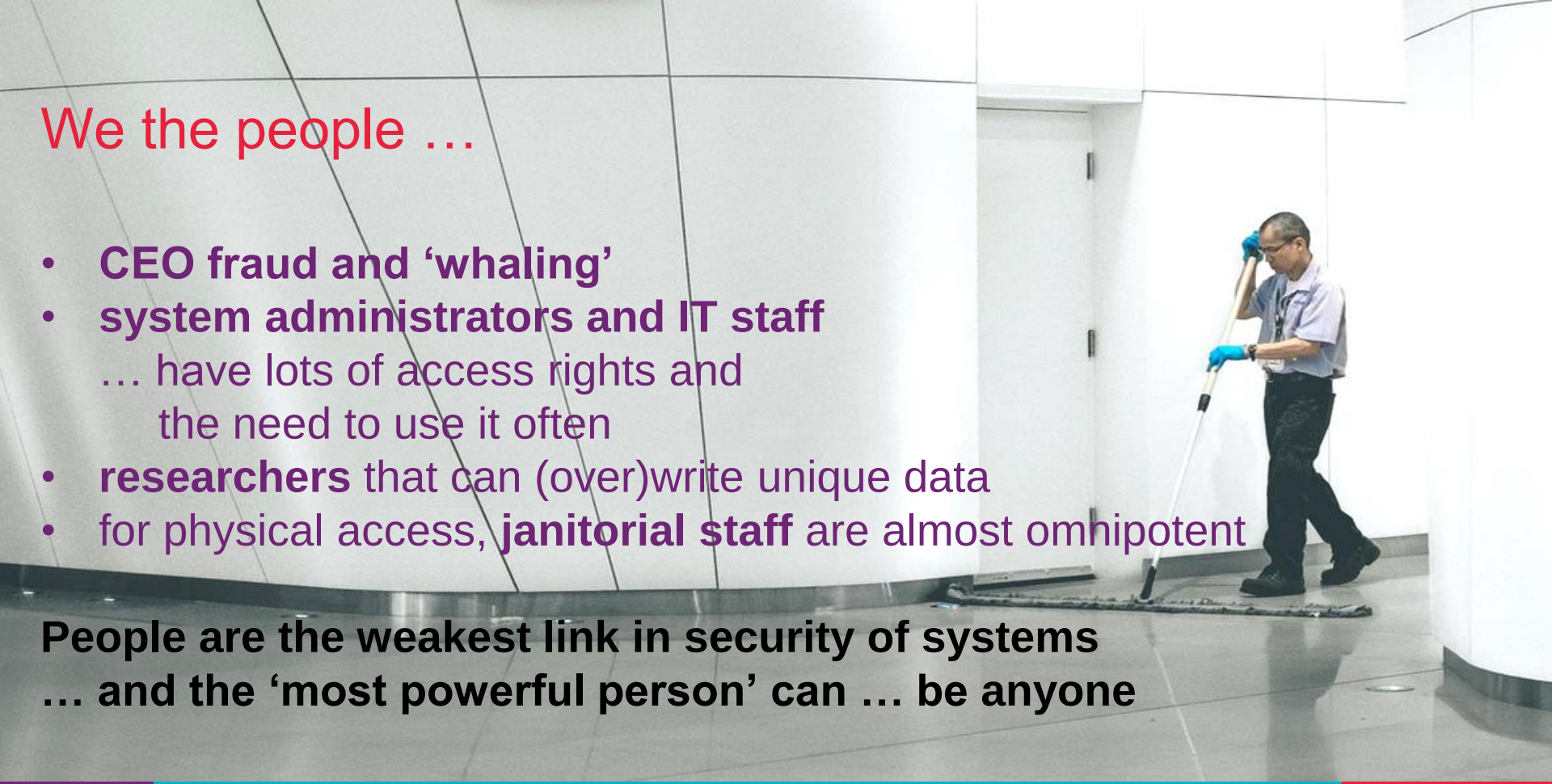
finding a bitcoin miner in an isolated ‘on-prem’ cloud?

network abuse to call many, expensive phone numbers??

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

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

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!

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.

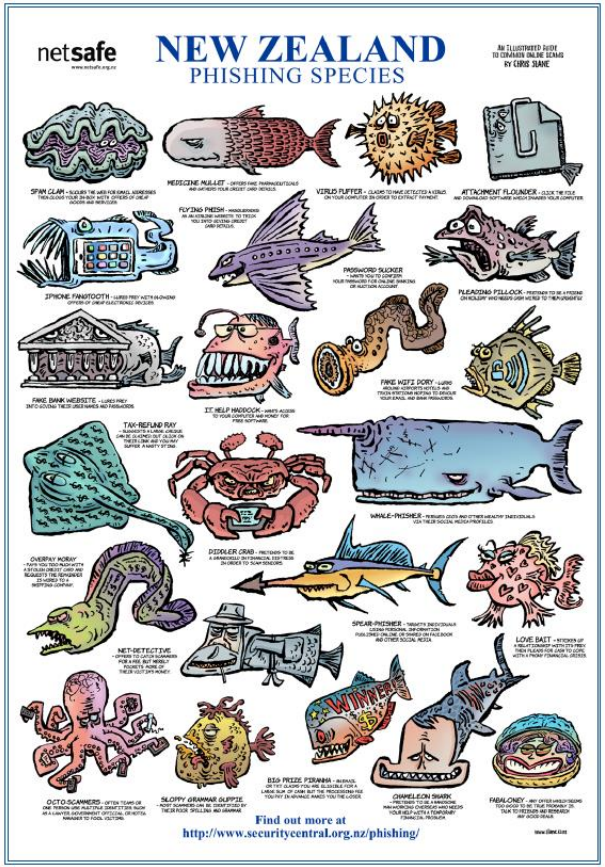
When it comes to phishing attacks, the Verizon team found that 23% of users open phishing emails and 11% take the extra PEBKAC step of actually clicking on the attachment. Even a small phishing campaign of 10 emails has a 90% chance of

is a mere one minute and 22 seconds.

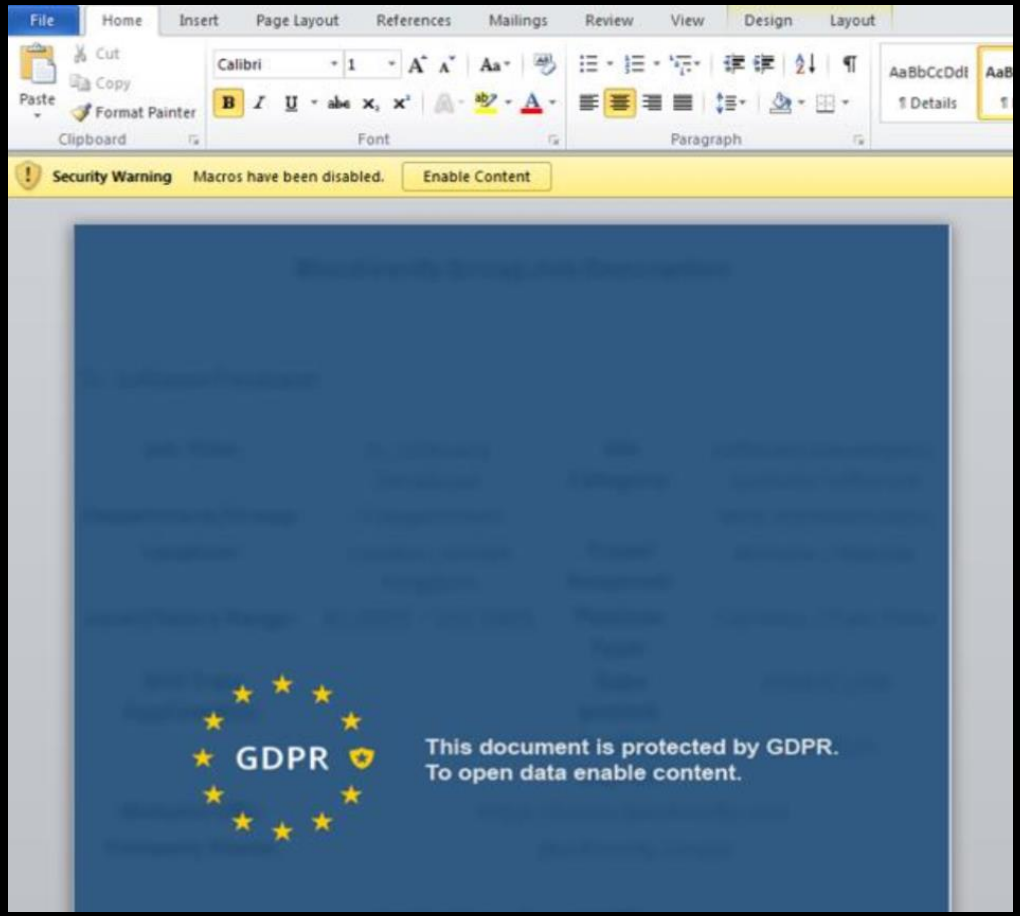
Don't forget to patch old vulnerabilities

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/



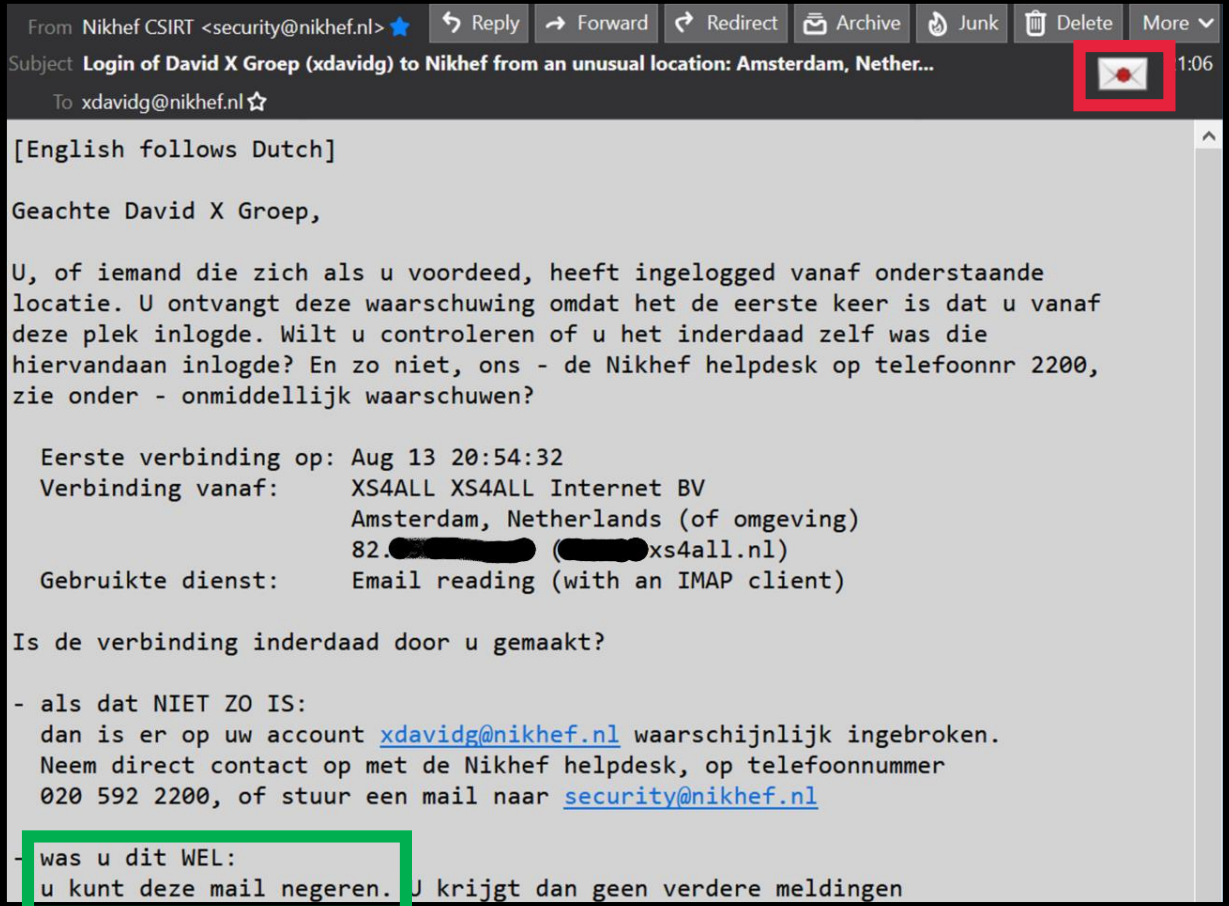
… of gewoon Emotet malware email
(van het Epoch3 kartel deze week)

FACTUUR J-192 van [naam]
Fact. 0680888 van [naam]
Fact. 2020-LIA20087 van [naam]
Fact. 613378 van [naam]
Factuur 08.2020-006073 van [naam]
Factuur 08.2020-MO463 van [naam]
Factuur 29754590 van [naam]
Factuur 9611-08.2020 van [naam]
Factuur HT93446652-2020 van [naam]
Factuur MG-43324 van [naam]
Factuur SNW007956800 van [naam]
Factuur van [naam]
Inv 0000209205 van [naam]
Inv 08.2020-wjh79734 van [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

Once the attacker is in – he lies in waiting …

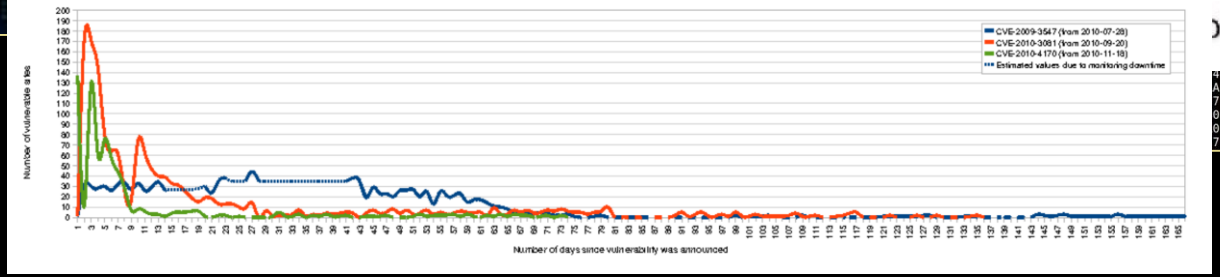
cp<r>

HEARTBLEED

```
00e0: 3B 71 3D 30 2E 38 0D 0A 41 63 63 65 70 74 2D 4C  ;q=0.8..Accept-L
00f0: 61 6E 67 75 61 67 65 3A 20 65 6E 2D 55 53 2C 65  anguage: en-US,e
```

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 netwerk toegang krijgen tot doel-systeem en malware uitvoeren met het lokale SYSTEM account.

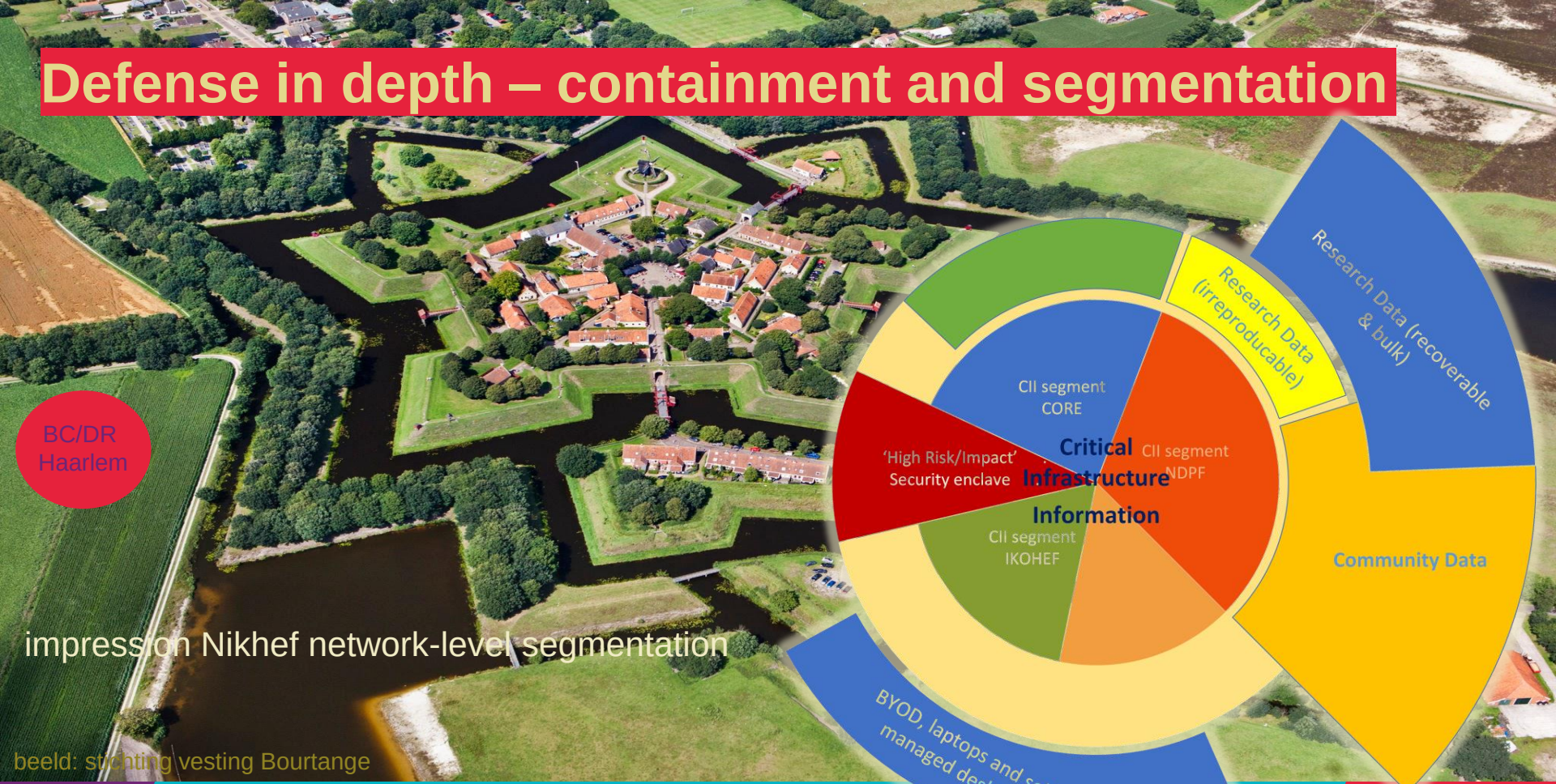
de server



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/

Defense in depth – containment and segmentation



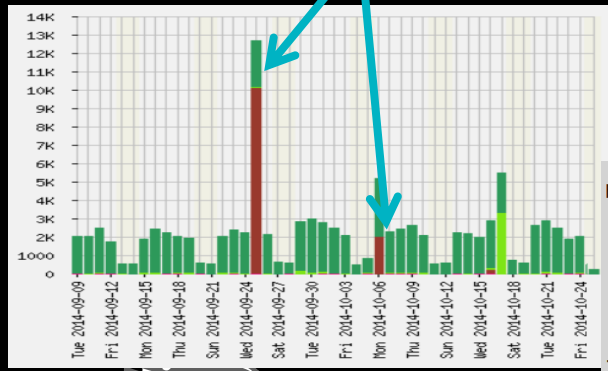
impression Nikhef network-level segmentation

beeld: stichting vesting Bourtange

Segmentation of access rights

Through phishing, outsiders and attackers will appear as insiders
So limit what an insider can do,
to what is needed … but don't go overboard

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)
```

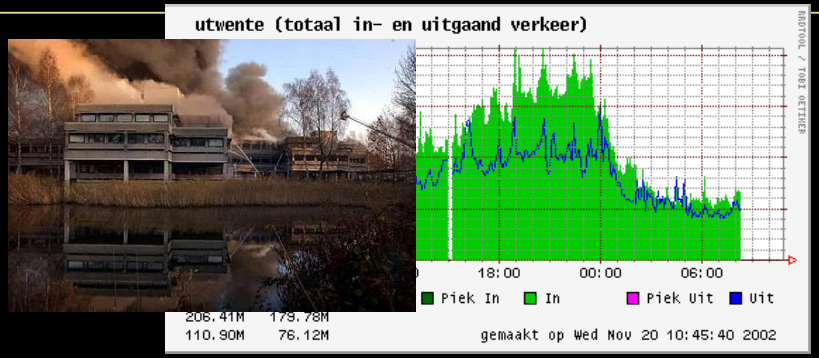


Image: PS control room at CERN

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

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?

if you suddenly find yourself in the news?

report to LE, or recover services?

trust and delegation for operational response?

‘Operational’ level – the Computer Security Incident Response Team: CSIRT

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

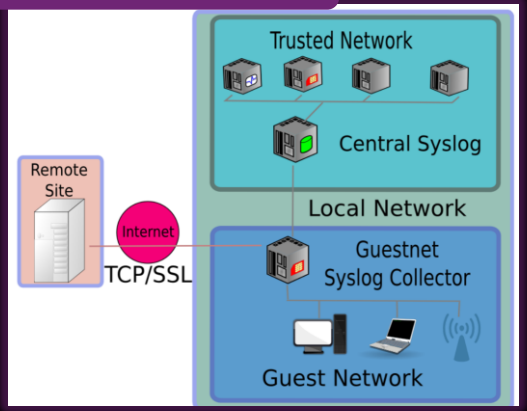
detecting something is weird in the first place

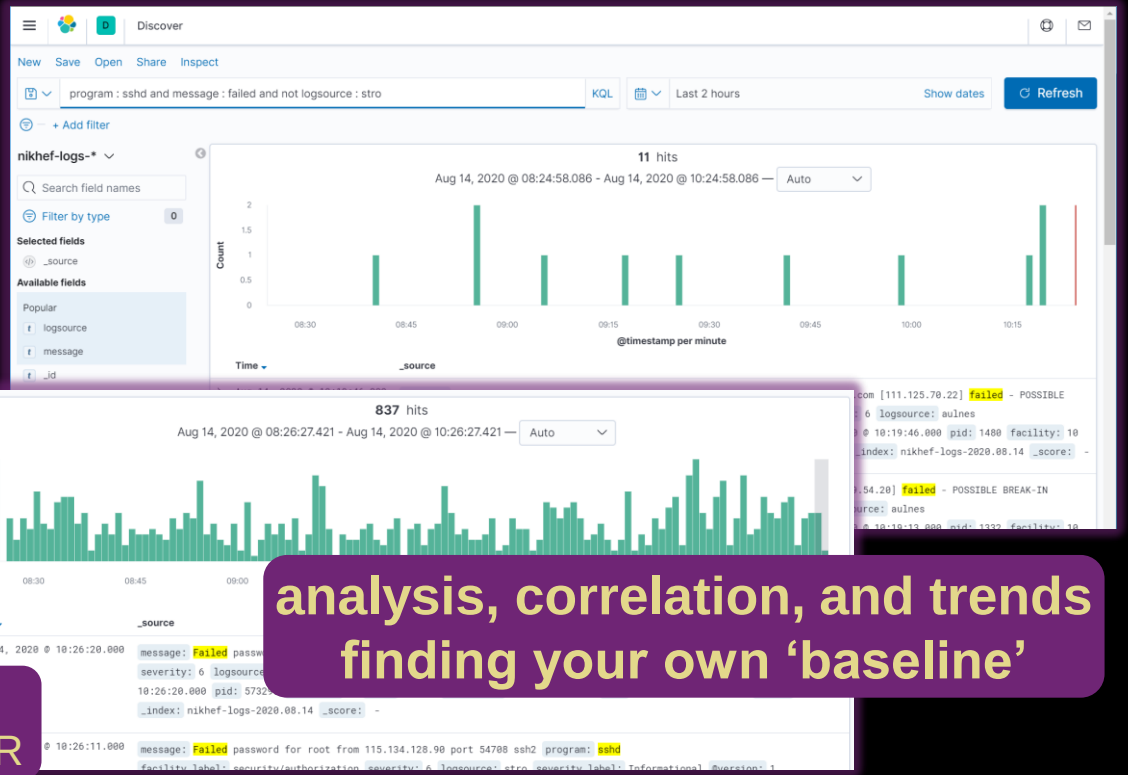
An attacker! … *… or maybe a PhD student?*

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

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

collection of data



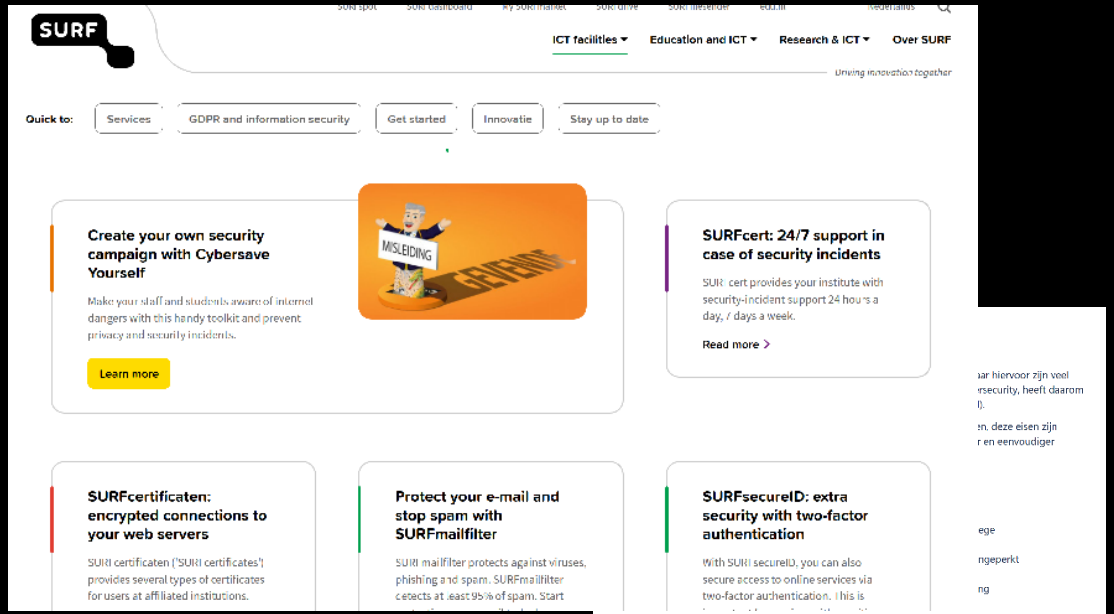


analysis, correlation, and trends
finding your own ‘baseline’

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

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, 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

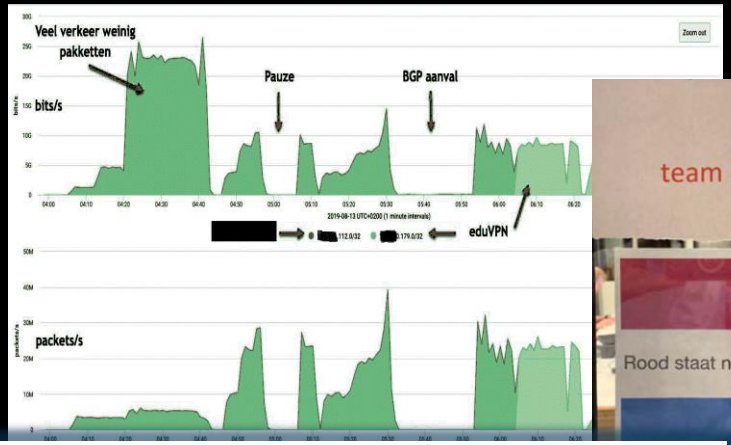
Trust groups

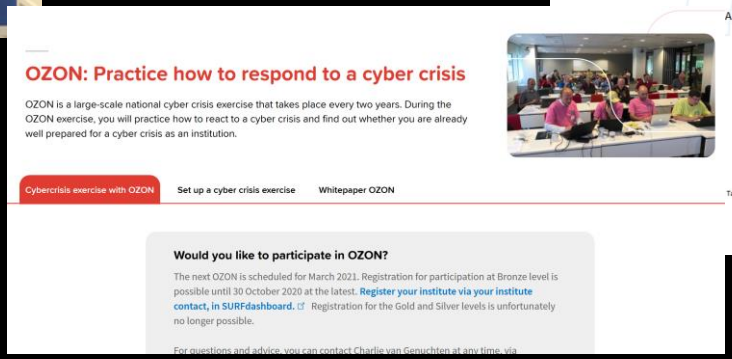
Beyond ‘organisational’ trust - contribute and participate …
… and you will reap the benefits in turn

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

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

Exercise! From technical, to federated, to strategic





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

source: www.krone.at

source: www.hessenschau.de

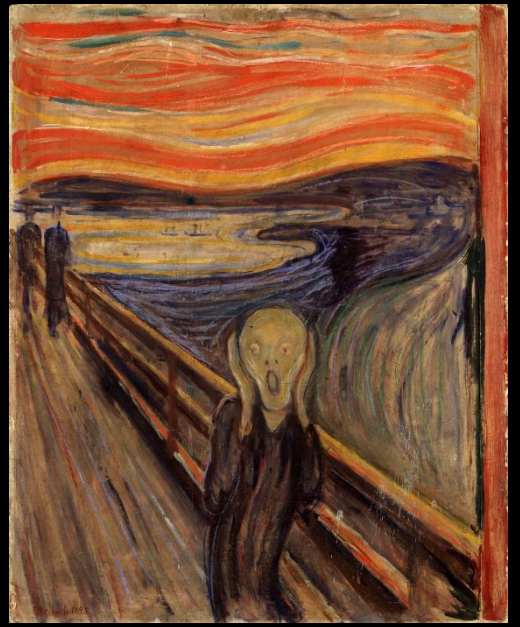
You hear that you're compromised … and now what?

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?

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

3. Be glad to have your operational security team
   in place & engaged …
   and if you, or they, get stuck, there is a community that can help you, including SURFcert and peers …



Any specific recommendations?

- **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

All material not otherwise attributed to third party sources is licensed under the Creative Commons Attribution License

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*

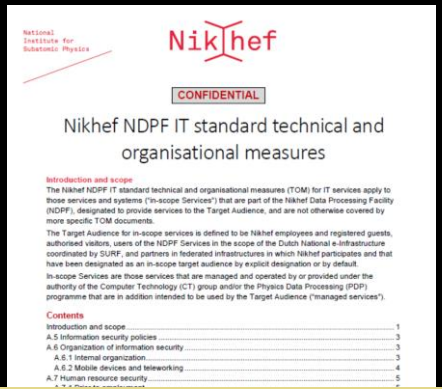
but all views are of course my own and not necessarily shared by any of them …

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

The Importance of Being Open – in Europe and beyond

Beyond a single organisation

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


Nikhef

CONFIDENTIAL

Nikhef NDPF IT standard technical and organisational measures

Introduction and scope

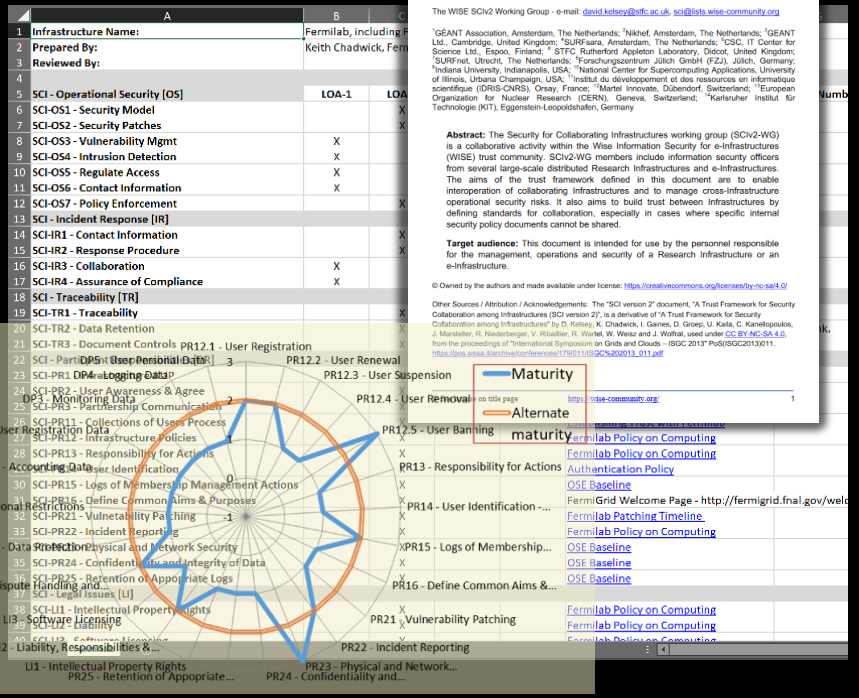
The Nikhef NDPF IT standard technical and organisational measures (TOM) for IT services apply to those services and systems ("in-scope Services") that are part of the Nikhef Data Processing Facility (NDPF), designated to provide services to the Target Audience, and are not otherwise covered by more specific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

Introduction and scope 1
A.5 Information security policies 3
A.6 Organization of information security 3
A.6.1 Internal organization 3
A.6.2 Mobile devices and teleworking 4
A.7 Human resource security 5



	A	B
1	Infrastructure Name:	Fermilab, including F
2	Prepared By:	Keith Chadwick, Fern
3	Reviewed By:	
4		
5	SCI - Operational Security [OS]	LOA-1
6	SCI-OS1 - Security Model	
7	SCI-OS2 - Security Patches	
8	SCI-OS3 - Vulnerability Mgmt	X
9	SCI-OS4 - Intrusion Detection	X
10	SCI-OS5 - Regulate Access	X
11	SCI-OS6 - Contact Information	X
12	SCI-OS7 - Policy Enforcement	
13	SCI - Incident Response [IR]	
14	SCI-IR1 - Contact Information	
15	SCI-IR2 - Response Procedure	
16	SCI-IR3 - Collaboration	X
17	SCI-IR4 - Assurance of Compliance	X
18	SCI - Traceability [TR]	
19	SCI-TR1 - Traceability	
20	SCI-TR2 - Data Retention	
21	SCI-TR3 - Document Controls	
22	SCI - Participant Responsibilities [PR]	
23	SCI-PR1 - Privacy Policy	
24	SCI-PR2 - User Awareness & Agree	
25	SCI-PR3 - Partnership Communication	
26	SCI-PR11 - Collections of Users Process	
27	SCI-PR12 - Infrastructure Policies	
28	SCI-PR13 - Responsibility for Actions	
29	SCI-PR14 - User Identification	
30	SCI-PR15 - Logs of Membership Management Actions	
31	SCI-PR16 - Define Common Aims & Purposes	
32	SCI-PR21 - Vulnerability Patching	
33	SCI-PR22 - Incident Reporting	
34	SCI-PR23 - Physical and Network Security	
35	SCI-PR24 - Confidentiality and Integrity of Data	
36	SCI-PR25 - Retention of Appropriate Logs	
37	SCI - Legal Issues [LI]	
38	SCI-LI1 - Intellectual Property Rights	
39	SCI-LI2 - Liability	
40	SCI-LI3 - Software Licensing	

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[3], R Quick[8], W Raquel[10], V Ribaillier[11], M Sallé[2], A Scicchitano[12], H Short[13], A Slagell[14], U Stevanovic[15], 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.

© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/

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

User awareness and engagement

Consistent messaging to users – from the IT dept, but *also* from comms & PR – and *no* links that require credential entry to be sent by email

engage users in jointly working on security (CERN campaign “Sec_rity is not complete without U”)

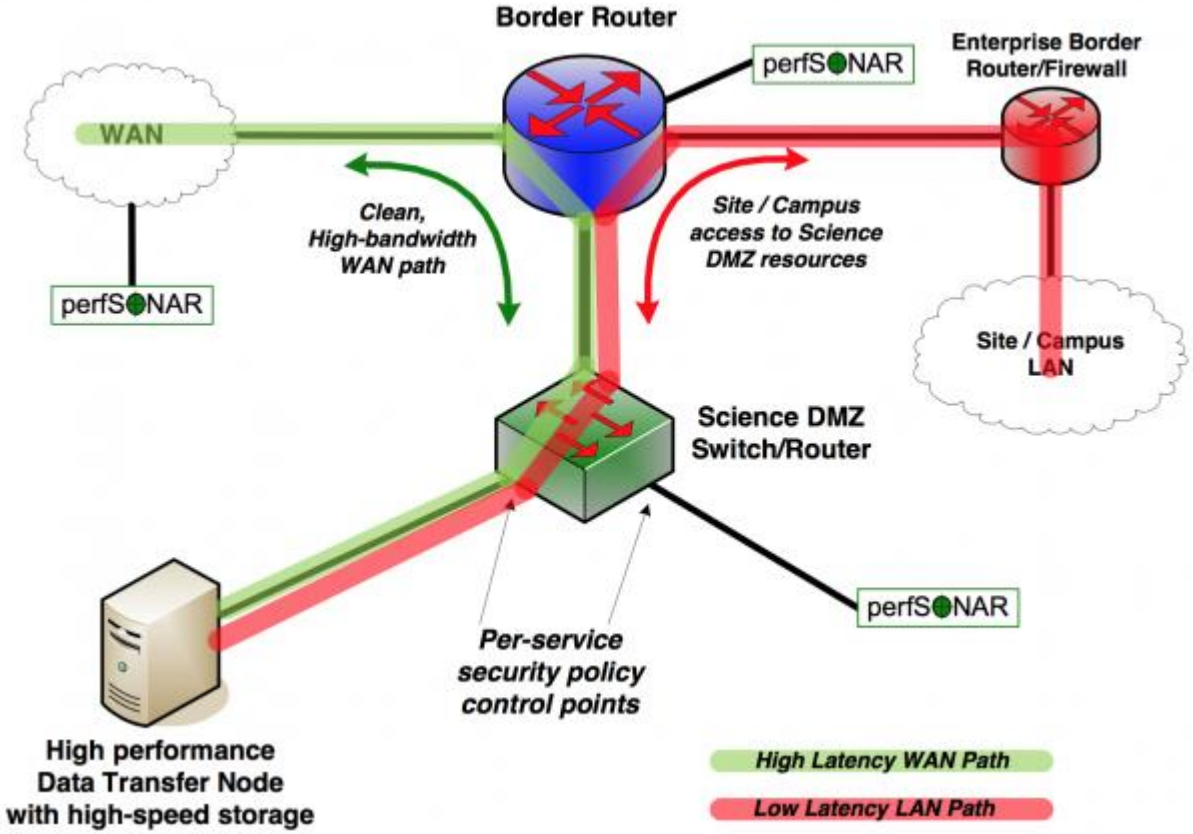
also means consistent SSO login as far as possible – one page only
(also helps in case you need MFA for additional assurance)
although we realise that in some cases you need direct entry of the same credential – then at least use consistent branding, and maybe training for EV checking

Use STITCH guidelines for evaluation/setting requirements for procurement

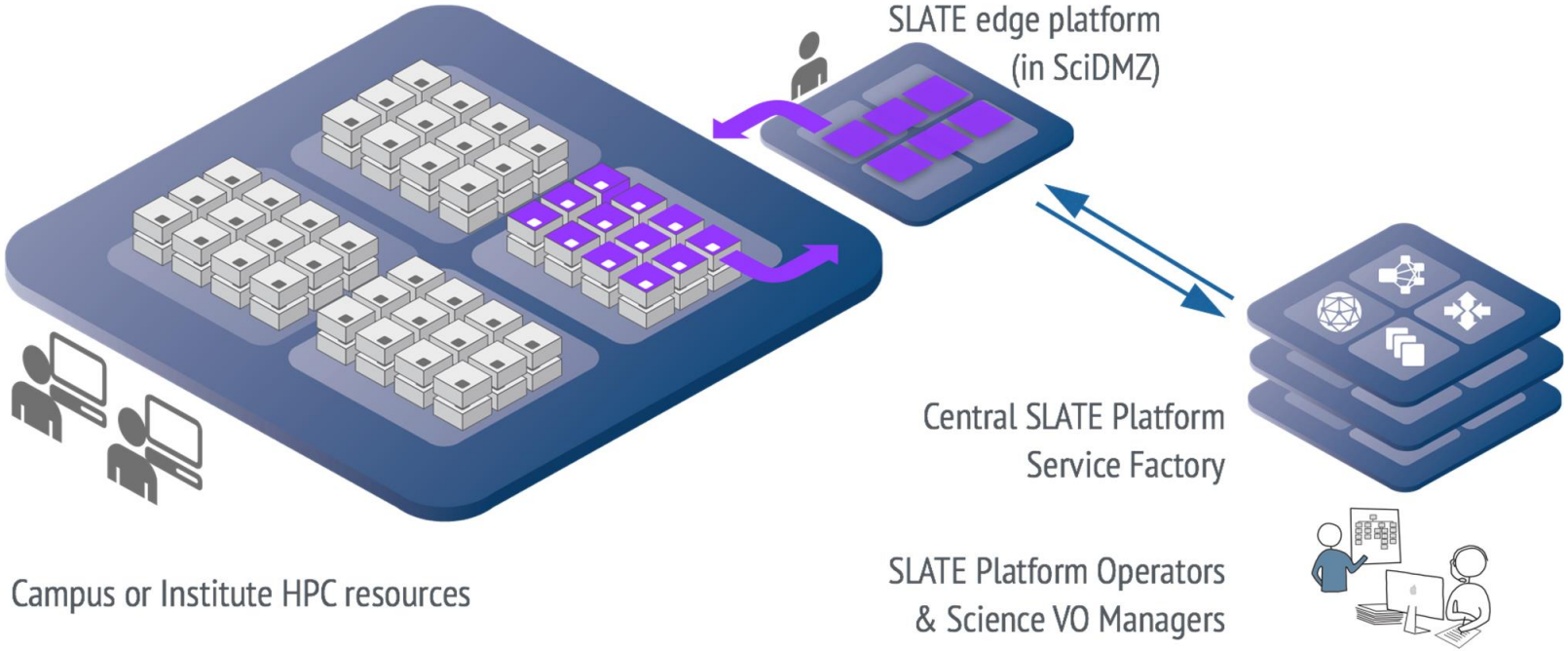
‘ScienceDMZ’

Network protection does mean cutting it off from the outside

remember that first presentation in the UM symposium …



SLATE CI


SLATE edge platform
(in SciDMZ)
Central SLATE Platform
Service Factory
SLATE Platform Operators
& Science VO Managers
Campus or Institute HPC resources

Segmentation: a research network with office enclaves

Example:
Nikhef high-level network

network is just one of a series of controls, alongside host-based controls, service-level controls, and object-identity-level controls

open-core implements the enclave structure, and allows open research federation

Segmentation of roles

The trivial basic: do not run with admin rights unless needed

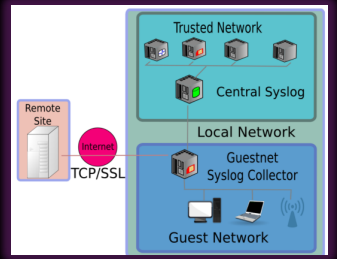
but it's easy to go overboard
with too many roles –
IGA should match the business needs

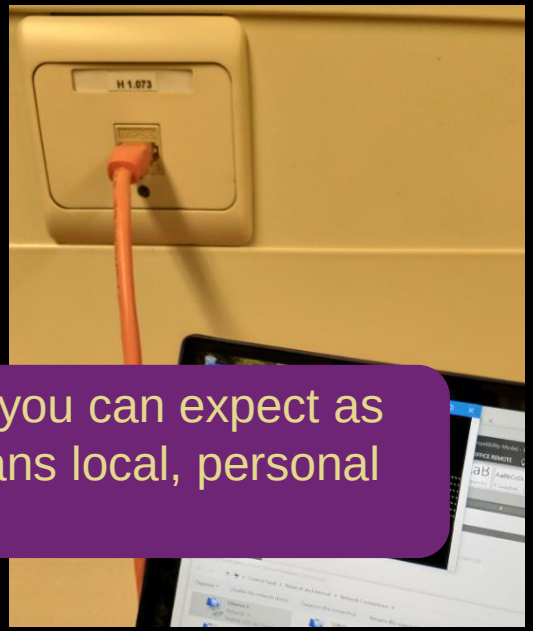
Example from a bank expanding into CEE, with ~700 employees and ~1400 roles – again: decide what actually needs protection, and where soft controls (awareness) are sufficient. Reduction to 200 roles made things significantly better, since now roles were actually manageable

Assets – you will know of some, you may never know all!

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

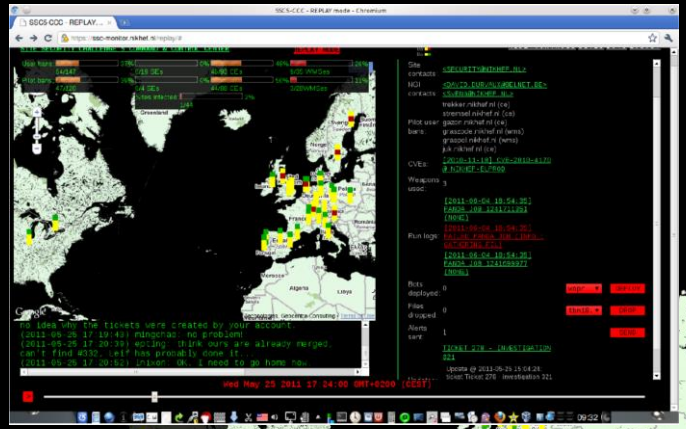




ge-3/0/22	ge-3/0/22	Patch H2.084 (H233)	cc:e1:7f			
ge-3/0/22.0	ge-3/0/22.0	ge-3/0/22.0	cc:e1:7f			
ge-3/0/23	ge-3/0/23	Patch H2.108 (H205)	cc:e1:7f			
ge-3/0/23.0	ge-3/0/23.0	ge-3/0/23.0	cc:e1:7f:8a:ef:1a		14, 49, 101	a0:1e:0b:03:27:dd (on vlan 14) dhcp-132-118.nikhef.nl (145.102.132.118) fe80::a21e:bff:fe03:27dd 2001:610:120:3001:a21e:bff:fe03:27dd

Know your users and what you can expect as ‘typical behaviour’ – this means local, personal knowledge

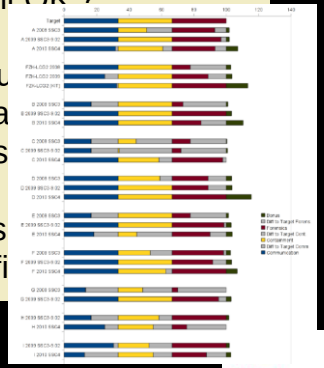
… the rest you test …



Communication:
- Endpoints valid?
- Form/Content OK ?

Containment
- Ban ”maliciou
- Find/Stop ma
- Find submiss

Forensics
- Basic Forens
- Network traffi



National Institute for Subatomic Physics

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!

BC/DR planning

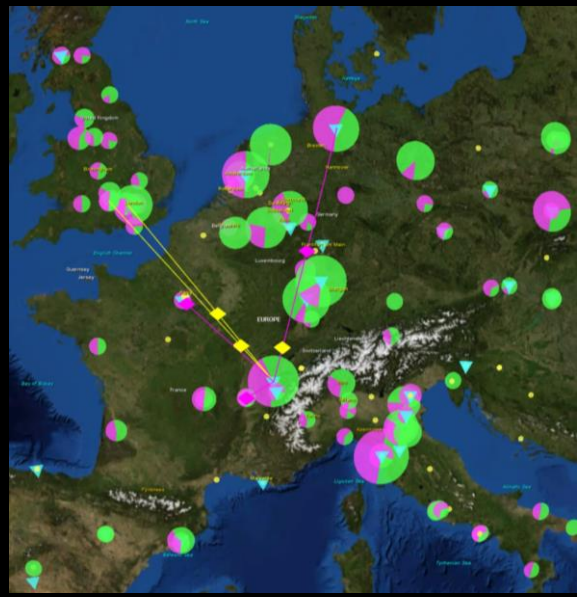
BC/DR can be at several levels – and doing it really well is very, very expensive
esp. the testing part, since if you *do* cover all aspects and you're not Tier-4 for both infra and services, it will be 'invasive and 'visible' to end-users

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

- make sure there are alternative 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

Business Continuity/Disaster Recovery – e.g. in our (redundant) LHC Tier-1 global network

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]

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

WLCG SOC WG

A SOC concept targeted at data intensive research

combine those elements of monitoring and capabilities that match the usage pattern, and scale to desired flows
(COTS/commercial SOCs will be all of our traffic as a DoS ☺)

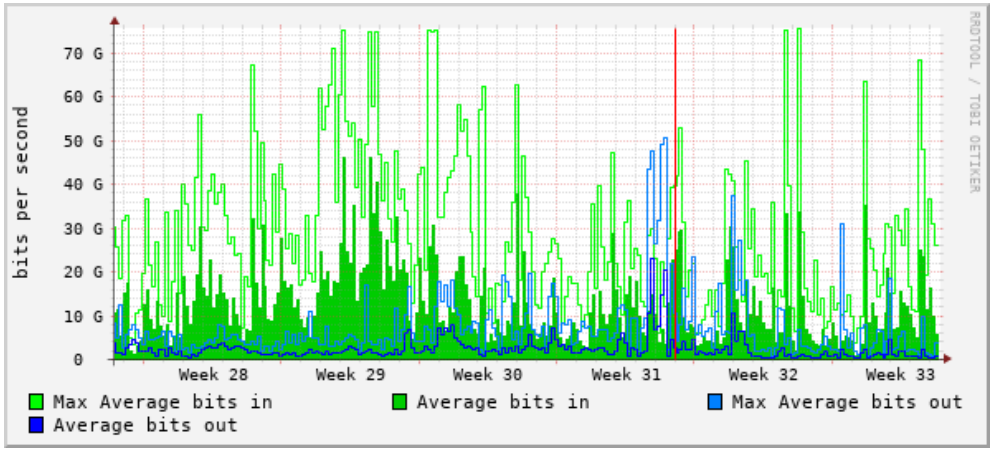
Leverage our community – our unique feature: MISP sharing of IoCs, trusted sources, contribute back

Zeek (f/k/a Bro) mirrored-monitoring of known IoCs
‘all we do must be stateless’

On COTS ‘commercial’ IDS firewalls and SOC offerings

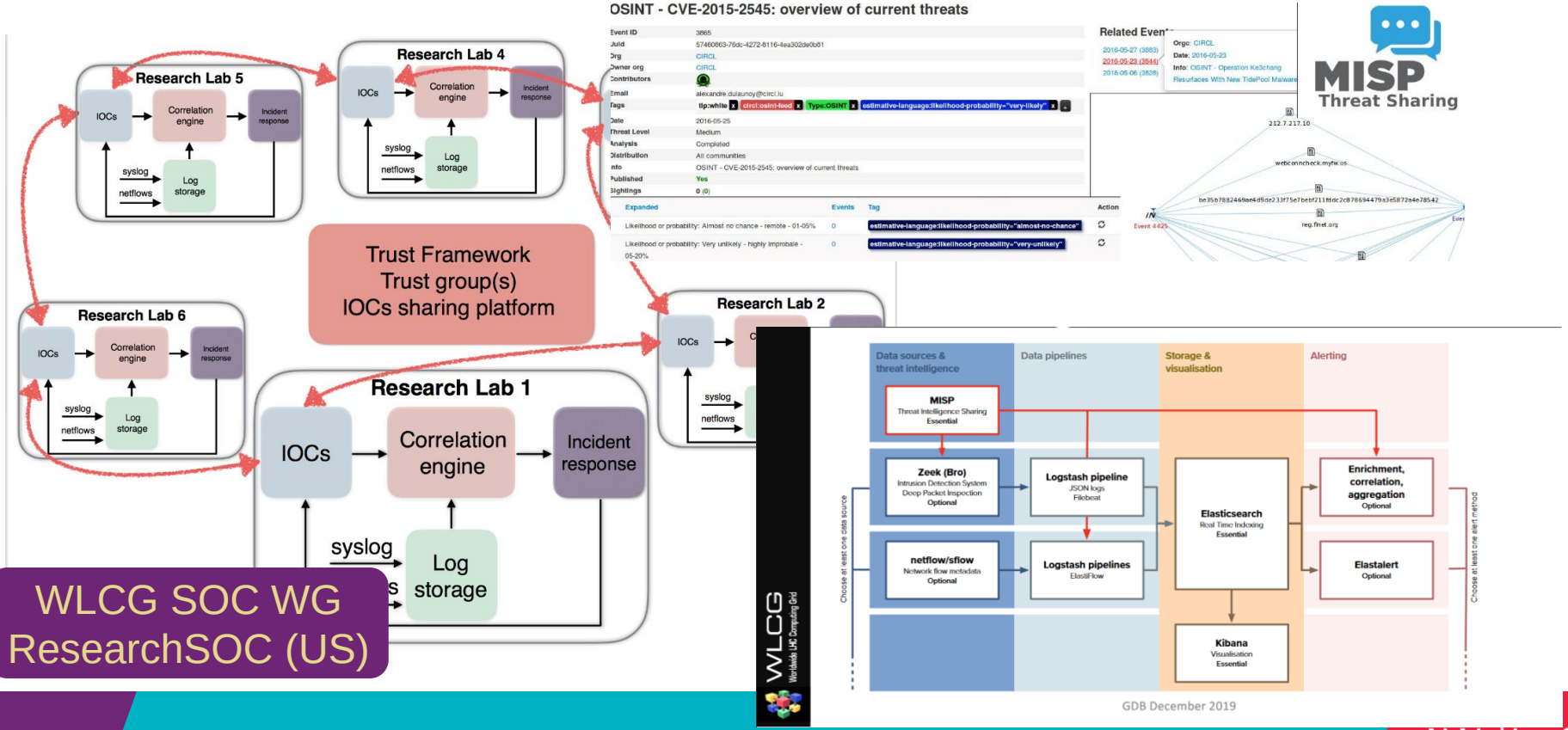
Commercial providers take care of some of the intel gathering for you but they do that for their ‘average’ customer, and will not see community, or research, specific threats or patterns

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

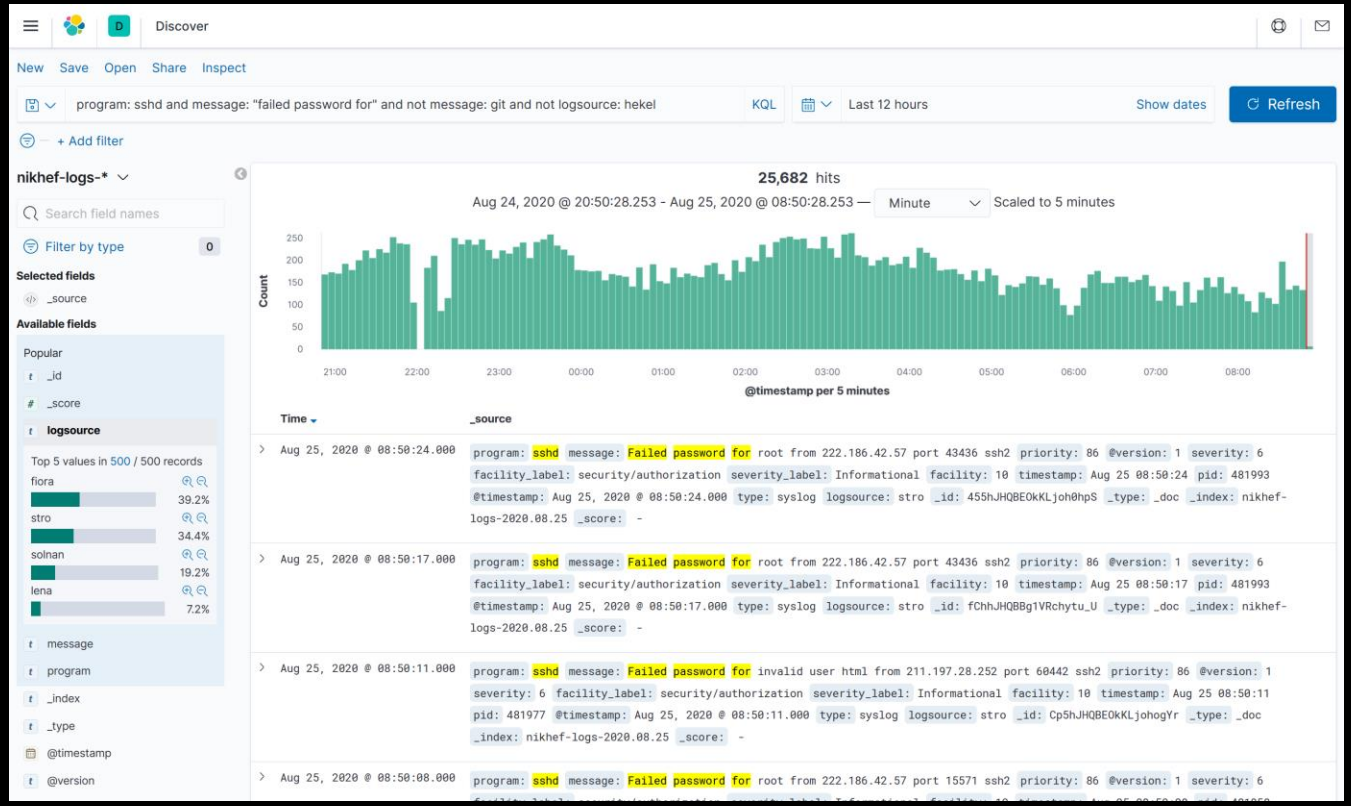


typical research network flow – Nikhef-SURFsara IC July-August 2020

Sharing threat intel – working with our community



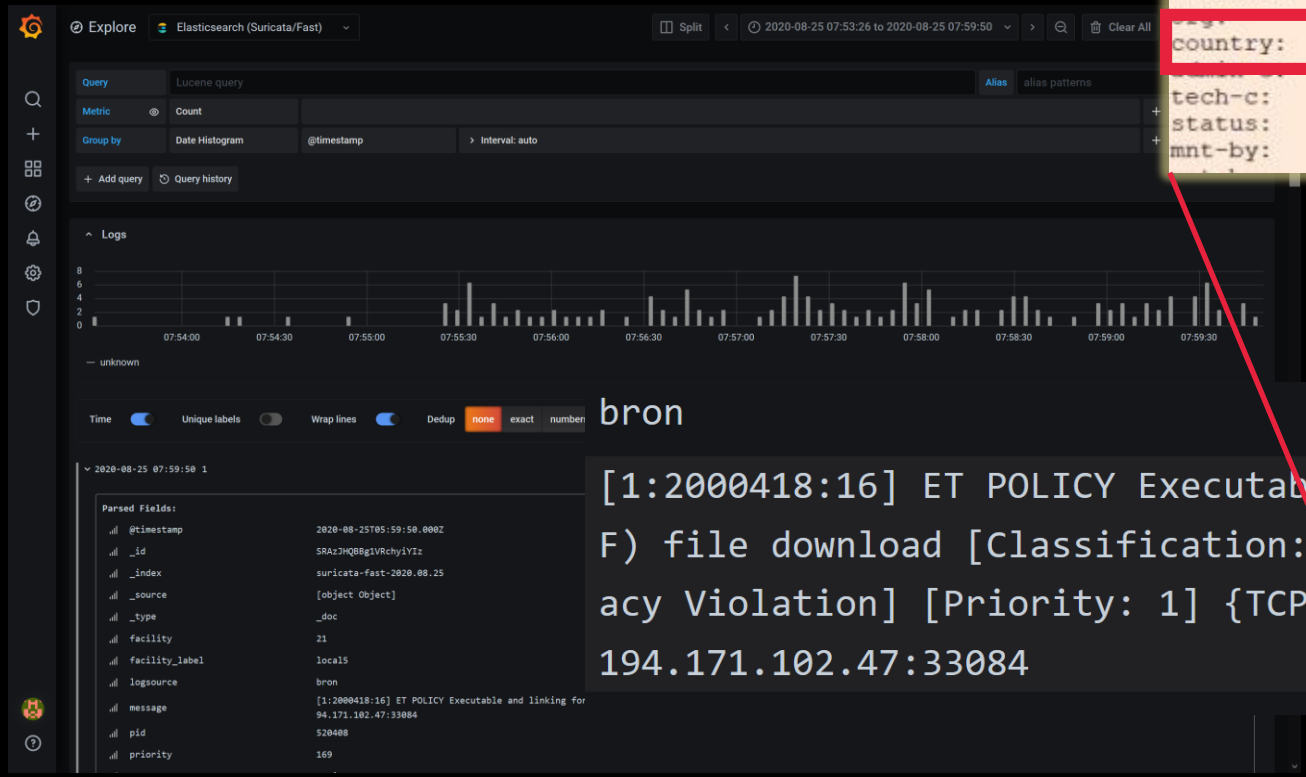
The marketing spiel: ‘we block 3000 attacks per hour!’



Nikhef SOC – NDPF traffic analysis

many ‘false warnings’: needs tuning

```
inetnum:        141.85.0.0 - 141.85.255.255
netname:        PUB-NET
                -PUB1-RIPE
country:        RO
                037-RIPE
tech-c:         GB6367-RIPE
status:         LEGACY
mnt-by:         RIPE-NCC-LEGACY-MNT
```



bron

```
[1:2000418:16] ET POLICY Executable and linking format (ELF) file download [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 141.85.240.238 1095 -> 194.171.102.47:33084
```

NikhefSOC/NDPF ELK setup: Jouke Roorda

Nikhef

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