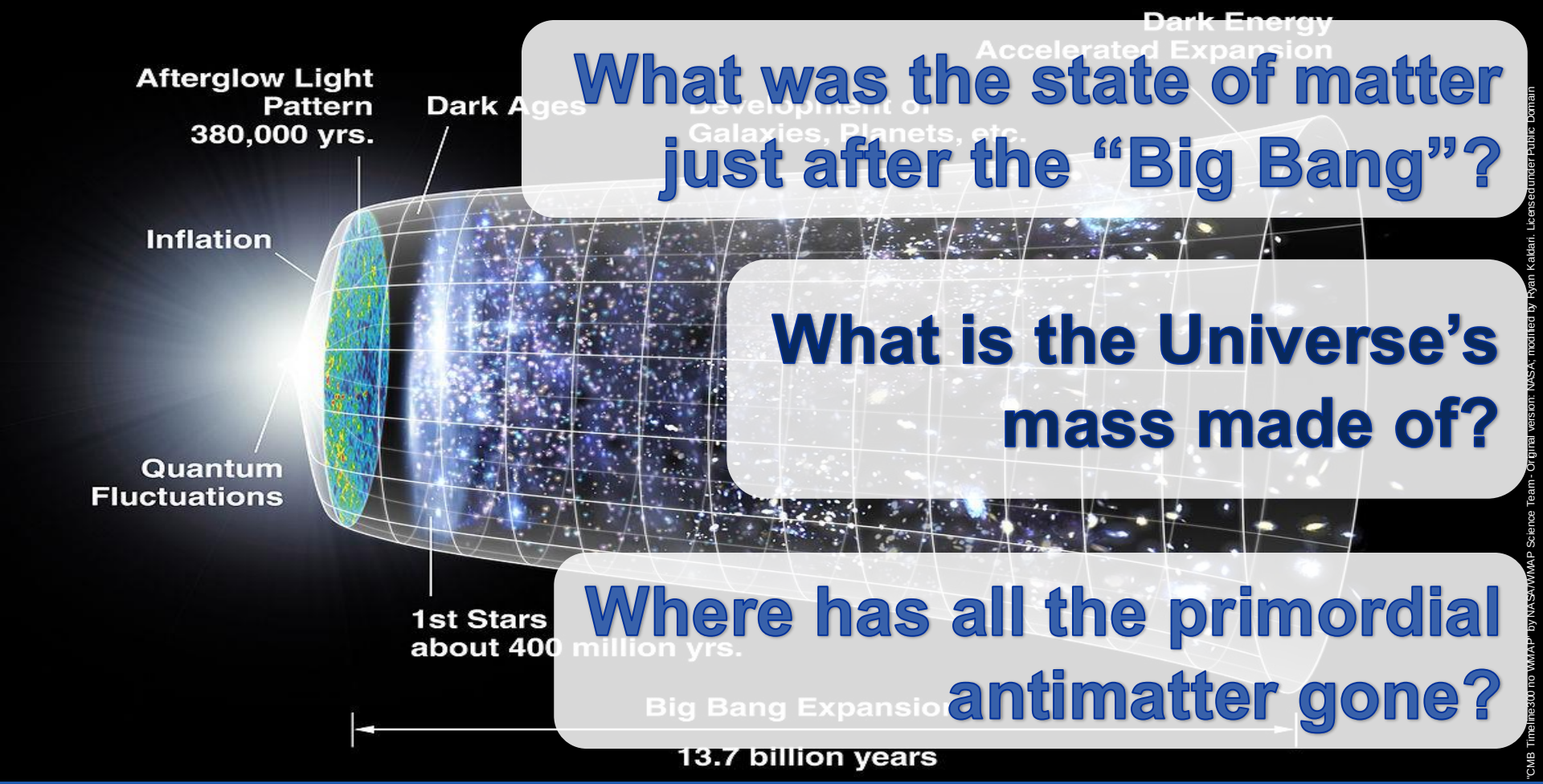
European Organization for Particle Physics

Exploring the frontiers of knowledge

My pick of
5 challenges
when protecting
Research & Education

Dr. Stefan.Lueders@cern.ch



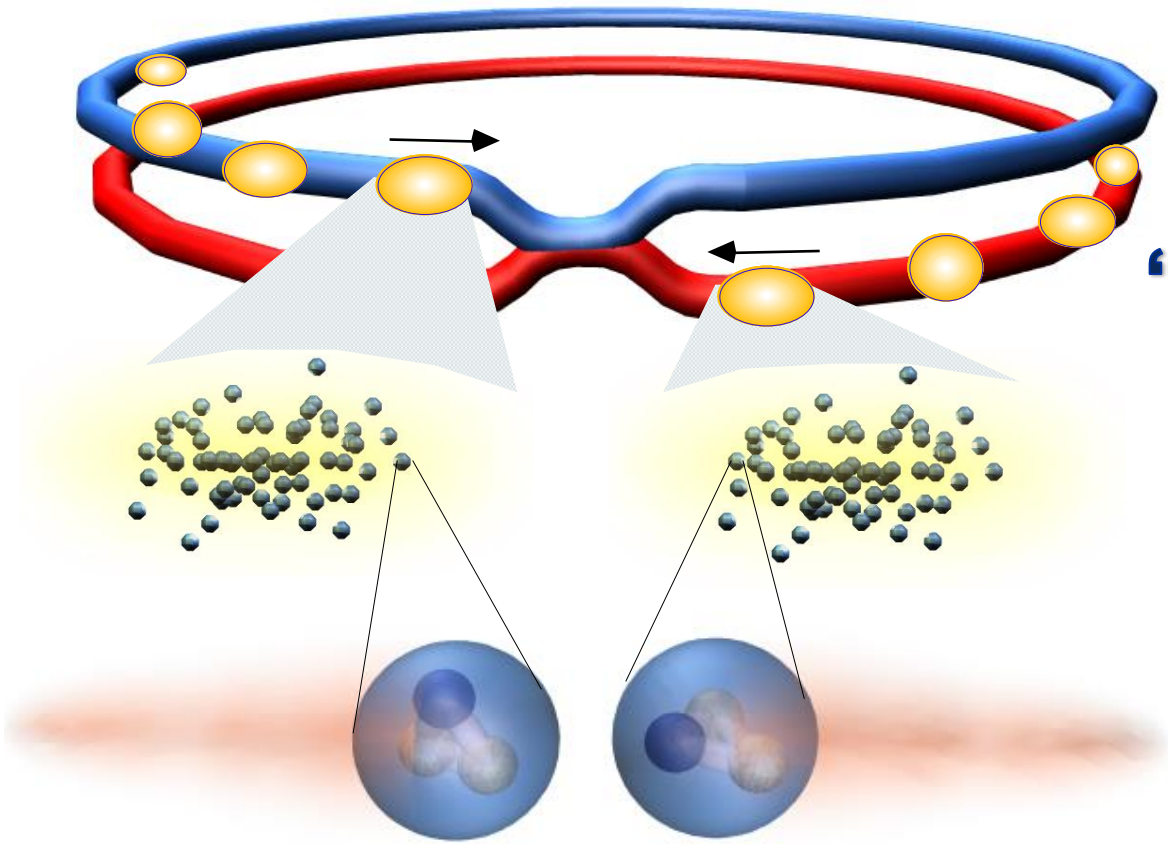
What was the state of matter just after the "Big Bang"?

What is the Universe's mass made of?

Where has all the primordial antimatter gone?

"CMB Timeline300 no WMAP" by NASA/WMAP Science Team - Original version: NASA; modified by Ryan Kaldari. Licensed under Public Domain

The Big Bang: 13.7B years ago

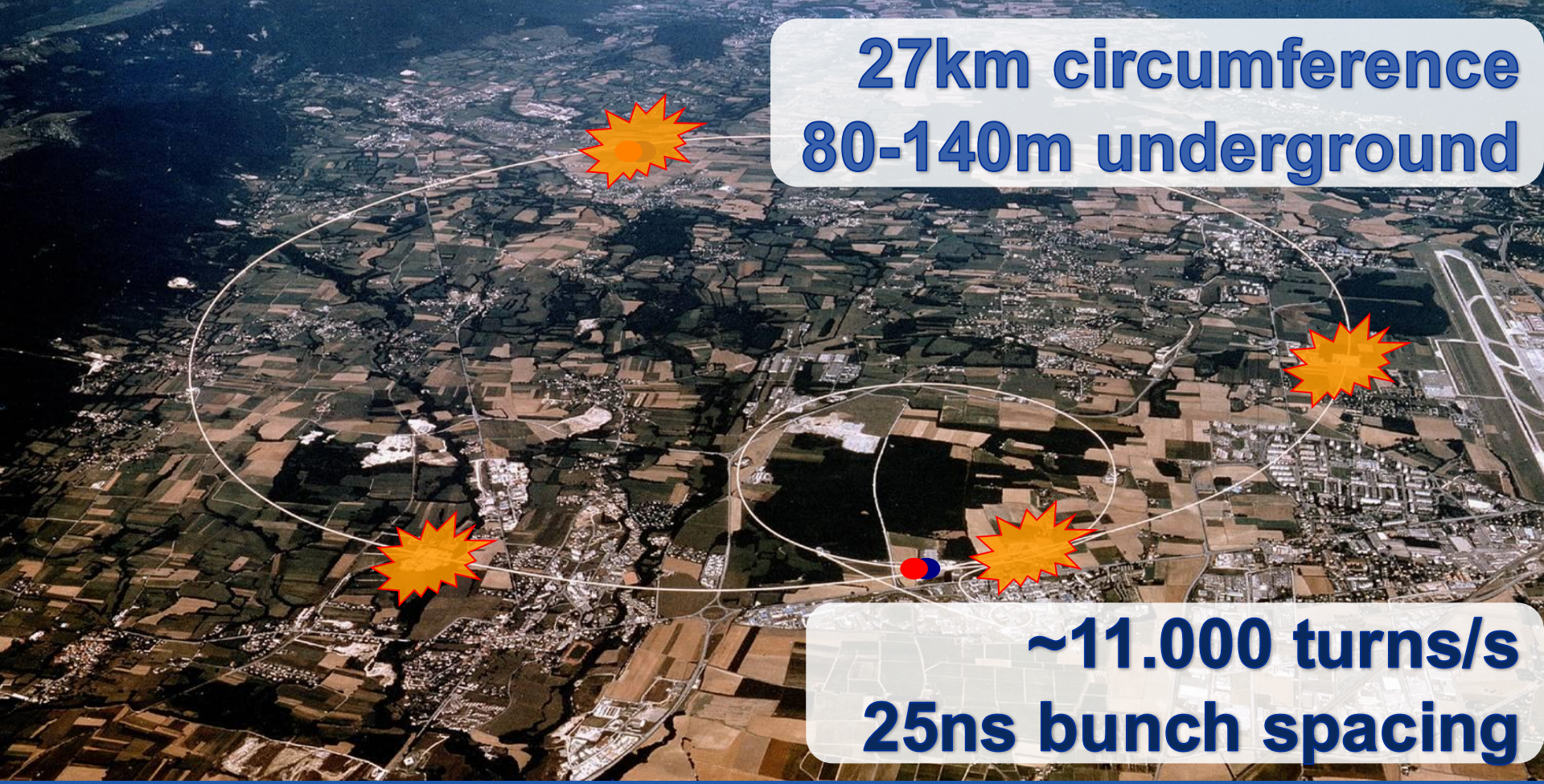


“Beam”: 2×2822b

“Bunch”: 10^{11}p

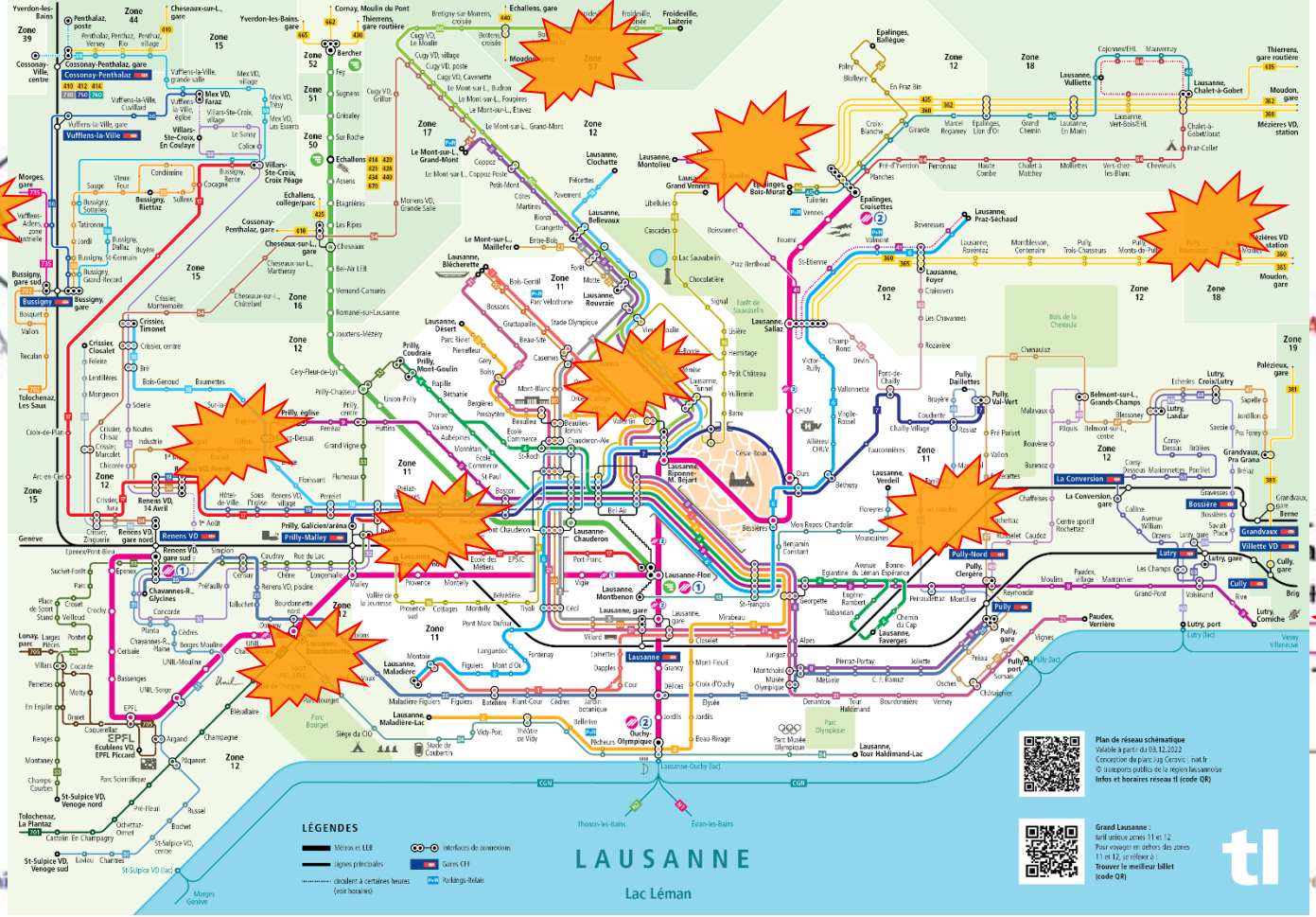
Protons/Quarks

Creating Big Bang Conditions

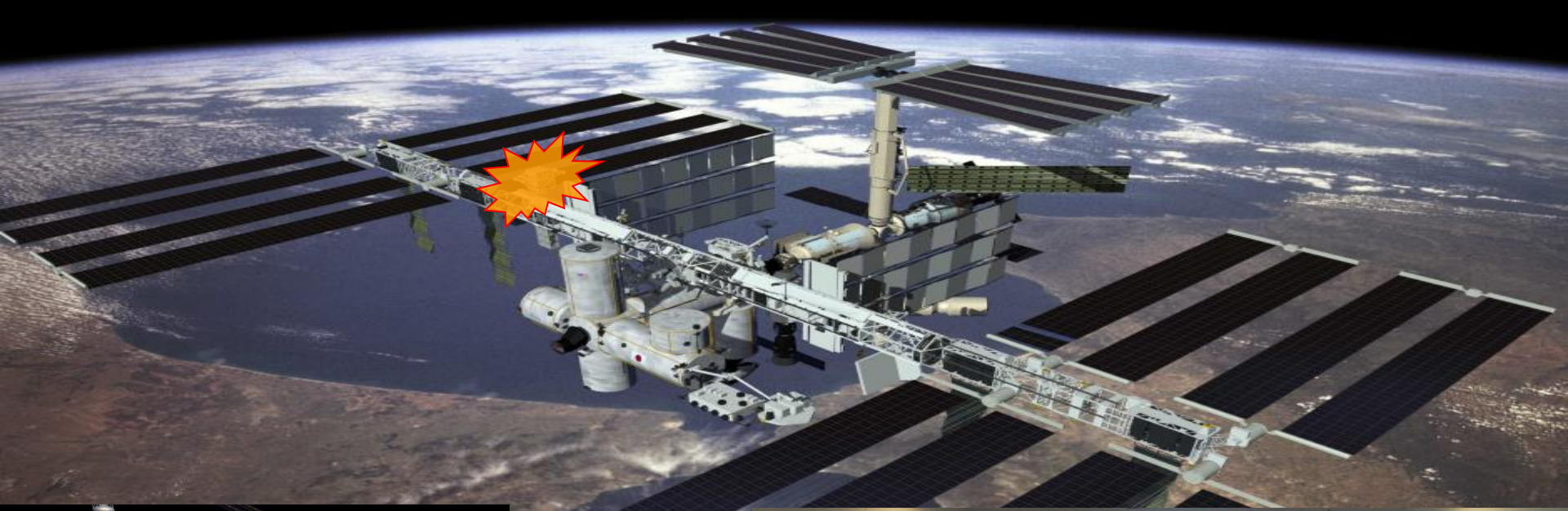


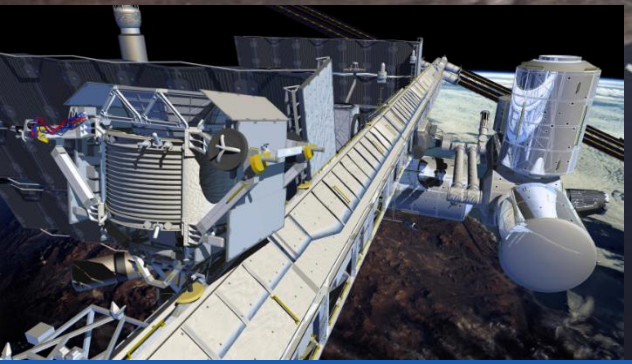
Dr. Stefan.Lueders@cern.ch
EPFL (CH), 2024/10/28

The Large Hadron Collider (LHC)



More than the LHC…





…and one detector in space

Four Sectors of Operation

One flat office, wireless & data centre network
(visitor laptops on par with
office PCs and data centre services)

5 Class-B IPv4 & 4 IPv6 networks
(+many non-routable networks)

160Gb/s backbone, >20 Gb/s flat bandwidth,
4000 switches, 300 routers, 6k firewall openings

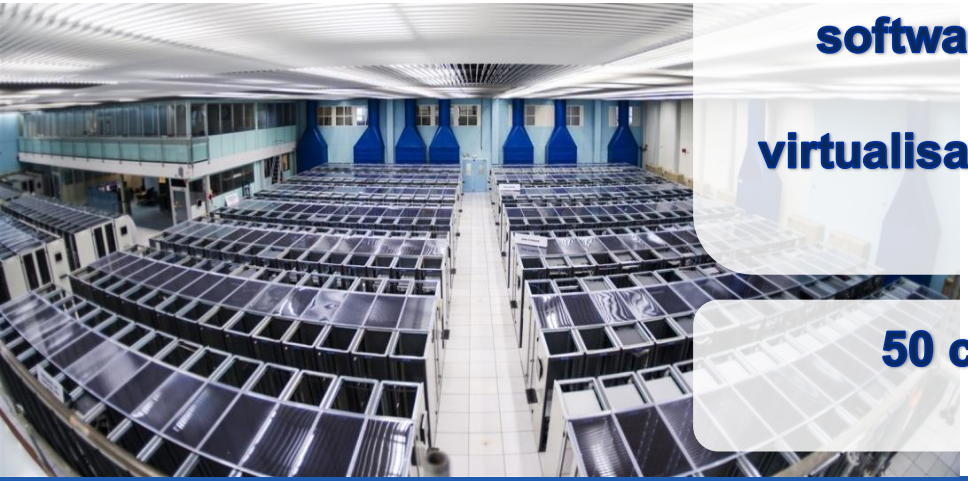
~271k heterogeneous devices registered:
any hardware, any operating system, any (legal) application

~37k user account & mailboxes, 2M emails/d

Office Computing Cyber-Security

7 data centres serving users, infrastructure, compute & storage, accelerators & experiments

~10k servers, 500k cores, 13k virtual machines,
~1EB storage (100k hard disks + 40k tapes)



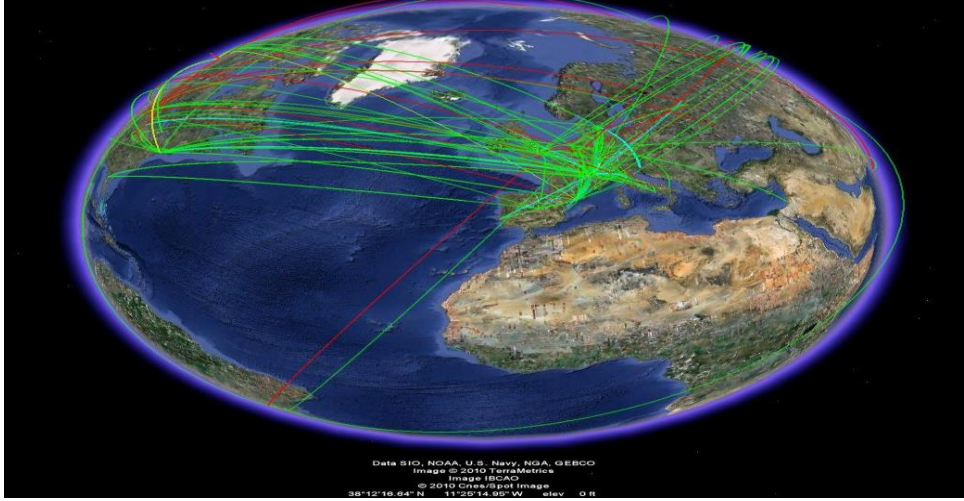
Provisioning of operating systems, printing, A/V software, office/engineering/HR/finance app's, data bases, versioning/build systems, virtualisation & container services, collaboration tools, video/audio conferencing, …

50 central + 500 decentral webservers, >10k websites, >1.5M webpages, webcast

Worldwide LHC Computing Grid (WLCG):

- Tier-0 (CERN: ~7k nodes)
- 13 Tier-1s, >150 Tier-2s and 3s

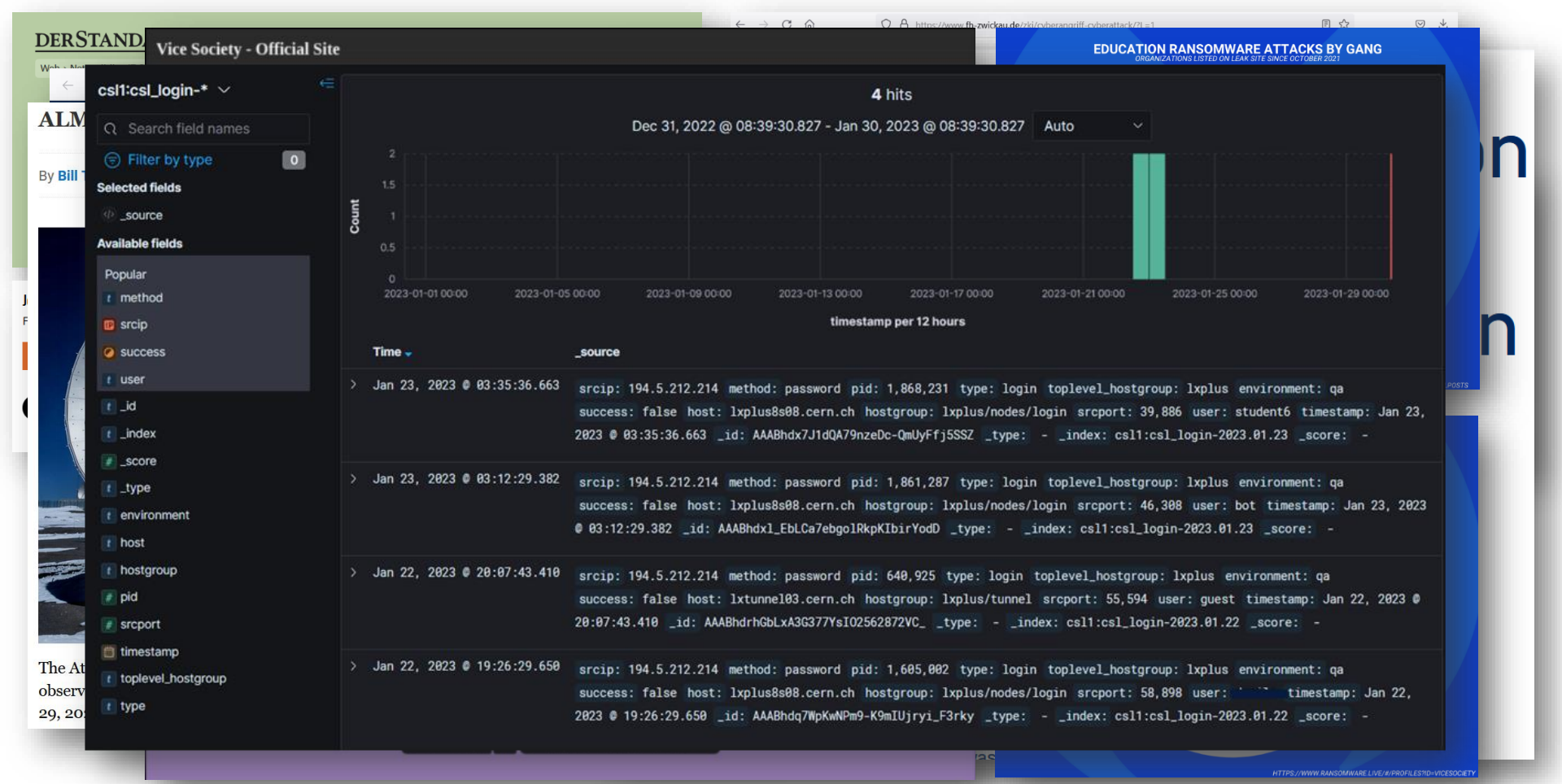
Permanently running >300k analysis jobs on ~1M CPU cores at >60Gb/s through-put



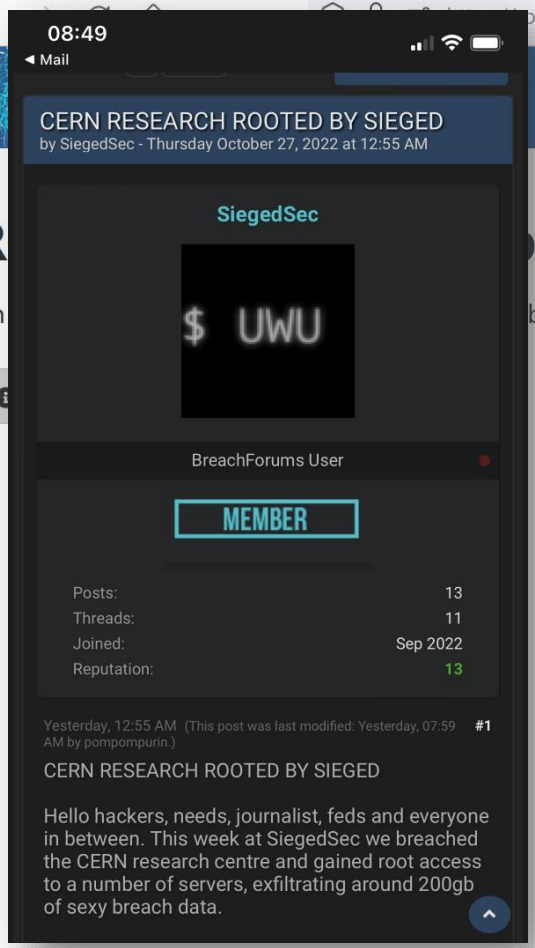
Adeli	Media-Lite SA
BIT (Swiss Confederation)	Opentransit (France Telecom Network Services Switzerland)
CERN	Orange Business Services - GIBN
COLT	RIPE-RIS
CTI	Sunrise (TDC Switzerland AG)
euNetworks (was Fibrelac)	Swisscom / IP-Plus
Init7	T-Systems Schweiz AG (Deutsche Telekom)
K-Net / K-Sys	UPC Cablecom
K-root (RIPE)	VTX Services SA
KPN Eurorings BV	

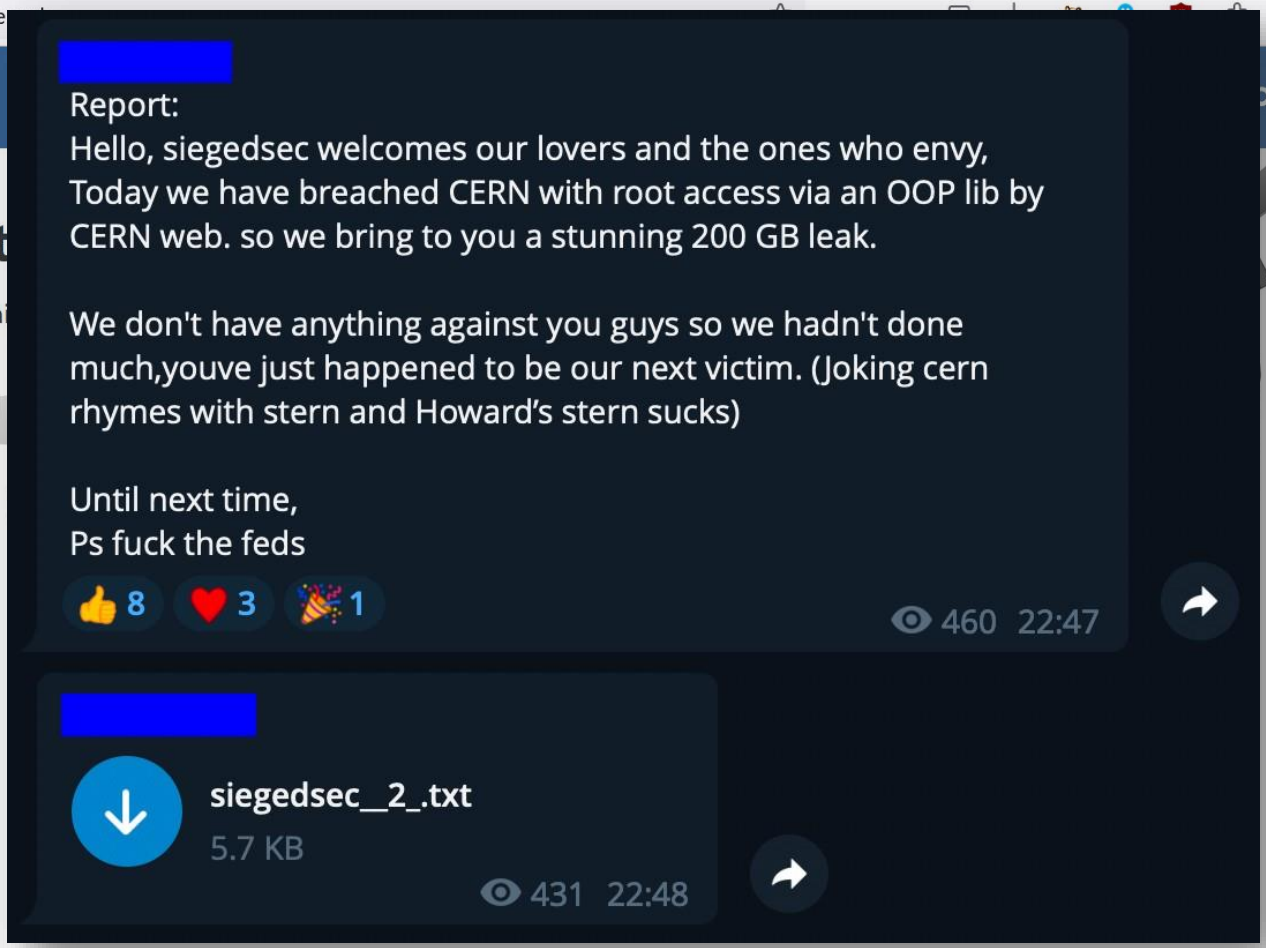
CERN Internet Exchange Point (CIXP):
20 Internet Service Provider (ISPs) & telecommunication companies

CERN's Academic Community



R&E has become target, too





Data Theft (…or not ☺)

Европейская организация по ядерным исследованиям под кураторством США, вторая по размерам в мире лаборатория физики высоких энергий. Также иногда переводится как Европейский Центр ядерных исследований. Аббревиатура CERN произошла от Conseil Européen pour la Recherche Nucléaire.

❌ Официальный сайт ЦЕРН
☐ https://home.cern/
https://check-host.net/check-report/cfa62c4ka78
❌ WEB Директория ЦЕРН
☐ https://directory.web.cern.ch/
❌ Авторизация для сотрудников ЦЕРН
☐ https://auth.cern.ch/
☐ https://login.cern.ch/

14.7K edited 06:28

KillMilk
Все отладили, всё работает. ЦЕРН без обид, ты был тестом🤦‍♂️

10.3K 18:50

KillMilk
Я так долго ждал этого дня ребята🥹

10.4K 18:51

Russian-speaking hackers knock multiple US airport websites offline. No impact on operations reported

By Greg Wallace, Sean Lyngaas, Pete Muntean and Michelle Watson, CNN
Updated 11:50 AM EDT, Mon October 10, 2022

DDOSsing CERN (for tests)

Governance

Computer Security Officer: Mandated by DG; generally *not* person responsible; independent in terms of decisions; part of IT management; ties with BC/DR lead, crisis management, Host Relations, legal, ODP, risk management, STEPS ("CIO")

Computer Security Team: 6 staff+students; many in-kind contributions and shared responsibilities with IT service managers (AD, EDR, firewall, IAA, …)

Standard: Audited 2023 against CISv8 (our choice)
82 findings (0 critical, 15 major, 33 moderate, 34 minor): no surprises, all expected; 50% under CSO, 50% under IT department/STEPS
https://www.cisecurity.org/controls/v8

Awareness, Training & Policies

Policies: Maintaining CERN Computing Rules (OC5). Improving governance and enforcement of "security".
https://cern.ch/ComputingRules

Basic Training: Giving regular awareness/on-boarding sessions. Plus online security courses. Plus "*Bulletin*" articles. Plus "clicking campaigns".
1+ session per month; 300+ articles published in total; 2k+ out of 22k+ people phished
https://security.web.cern.ch/training/en/CERN%20Articles%20On%20Computer%20Security.pdf

Dedicated Training: Providing in-depth training on security practices incl. programming. Plus "*Serious Gaming*" and "*WhiteHat Challenges*".
5 "*Zebra*" table-top exercises, one with real policemen from Geneva & Pays de Gex; ~100 CERN *WhiteHats* trained, plus many more students from external universities
"Thanks for cleaning up" – Bulletin article to come

Account Protection

2FA: Deploying extra protection to SSO/SSH.
9500+ accounts already enrolled. More to come
https://home.cern/news/news/computing/computer-security-log-click-be-secure

"*Gotham*": Notifying "unusual" logins.
~4770 notifications per month
https://home.cern/news/news/computing/computer-security-your-remote-logins

Dumps of Exposed Passwords: Notifying when used outside. Ditto for our community. Forcing reset when used at CERN.
Monitoring ~9k communities; reporting ~11k exposed passwords per day (~4/day for CERN)
https://home.cern/news/news/computing/computer-security-password-revolutions

Endpoint Protection

***EOP – xorlab – MDO* eMail-Filtering:** Quarantining SPAM & malware.
~115k analyzed per day; 10% SPAM; 2% quarantined; >12/d manually checked (MDO: >50% FP)
https://home.cern/news/news/computing/computer-security-fighting-spam-boss-level

***ESET* Anti-Virus/Anti-Malware:** Providing endpoint detection & response software for BYOD and CERN-owned devices.
~600 Bring-your-own-devices (BYOD) and 200+ CERN-managed devices
https://home.cern/news/news/computing/computer-security-winter-season-virus-time-one-free-pill-youl-device

***Threatray* Memory Hashing:** Detecting anomalies on CERN-managed devices.
~5500 CERN-managed devices enrolled

PenTests, Reviews & Consulting

Automatic Vulnerability Scanning: Identifying weaknesses of endpoints & servers, unused firewall openings, as well as exposed secrets.
~24k devices scanned per month; ~210 issues per month
https://home.cern/news/news/computing/computer-security_time-spring-clean

Security Consultancy & Reviews: Improving CERN's security posture (via *Cloud/Software License Office, IT consultants, IT Architecture Review Board*).
20-30 in-depth reviews per year

Self-Security Assessment for Cloud Services: Providing metrics, guidelines & controls for better security.
Based on CISv8 standard. Prototype ready. Web-portal in development

Network Protection

***PaloAlto* Firewalling:** Performing deep packet inspection and policy-based IP, domain & URL blocking.
>2x 200Gbps (ingress+egress) IPv4&v6 monitored in-line
https://home.cern/news/news/computing/computer-security-cerns-new-first-line-defence

DNS RPZ & Firewall: Blocking malicious & typo-squatting domains (with SWITCH). Ditto for 50+ CH & F hospitals.
~800 domains blocked by CERN, >100/day by SWITCH. No hospital got ransomwared so far
https://home.cern/news/news/computing/computer-security-when-cernch-not-cern

pDNS Containers: Helping WLCG sites to do alike.

Software Security

Code / Container Scanning: Deploying *GitLab/GitCI* and *Harbor* security features (SAST/DAST/…).
https://home.cern/news/news/computing/computer-security-avoiding-salmonella-your-code

Software-Bill-of-Materials (SBOM): Pushing for a curation service to avoid (automatic) downloading of malicious libraries, packages, containers & VMs. Document dependency trees and license constraints.
https://home.cern/news/news/computing/computer-security-when-your-restaurant-turns-sour

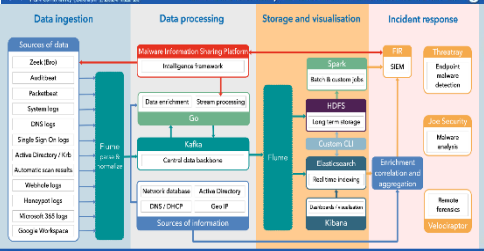
Threat Intelligence

ThreatIntel: Obtaining high-quality Indicators of Compromise.

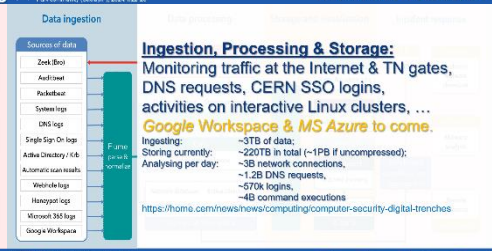
e.g. IPs, domains, file hashes from our peers and *Prodaft*, plus the *IWF* on CSAM (child sexual abuse material).
~15M IoCs shared with 1000+ peer organizations; 100k+ IoCs currently actively monitored
https://home.cern/news/news/computing/computer-security-protective-intelligence

Collaboration: Acting as a trusted, neutral broker, aiming at fostering cooperation and trust in our community: *WLCG/EGI/OSG*, *SWITCH* (CH), *REN-ISAC* (5-eyes); +Governments: *MELANI* (CH), *ANSSI* (F), *CH-CERTs*; +Law enforcement: *Interpol*, *Europol*, *FBI*, *CISA*, local police; +Int'l org's: *GISSIG/UNISSIG*; and with security vendors.
P.ex. 120+ universities world-wide notified this year of ransomware preparations in their IT infrastructure

Orchestration (the "SOC")



Intrusion Detection



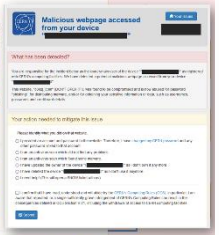
Ingestion, Processing & Storage: Monitoring traffic at the Internet & TN gates, DNS requests, CERN SSO logins, activities on interactive Linux clusters, … *Google Workspace & MS Azure to come.*

Ingesting: ~3TB of data;
Storing currently: ~220TB in total (~1PB if uncompressed);
Analysing per day: ~3B network connections, ~1.2B DNS requests, ~570k logins, ~4B command executions
https://home.cern/news/news/computing/computer-security-digital-trenches

Incident Response

"*Auto-Notify*": Notifying resource owners (devices, accounts, websites, …) of problems with their resources.
~300 reports per month (plus ~4700 "*Gotham*")
https://home.cern/news/news/computing/computer-security-our-findings-your-problem

Forensics: Providing capabilities and tools like *Prodaft*, *Threatray*, *Velociraptor*.
https://home.cern/news/news/computing/computer-security-catch-me-if-you-can



CERN & HEP CSIRT

CERN Computer Security Rota: Providing 2nd line Guys-on-Duty ("GoD"); 3rd line Security Escalation Cordinator ("SEC"); 4th line Computer Security Officer.
~150 SNOW and ~36 FIR tickets handled per month; 5-10 "heavy" incidents per year

Grid Security Rota: Leading the WLCG Security Office; Leading *EGI* Incident Response Taskforce; Leading *EOSCfuture* Incident Response TF.

"*SAFER*" Community Security: Providing world-wide incident response.
https://home.cern/news/news/computing/computer-security-safer-teamwork

A Comprehensive Porte-Folio

5 challenges when protecting Research & Education

I would like to keep SSO as now.

I am not able to use 2FA,to complicate for me

1. Does the 2FA switch concern all users of the

CE

se

I've got a lot of problems

1) I have no regular experience in scanning the QR code on the phone.

How l

screen

should

proce

I am following the instruction to activate 2FA. For this I need to download the Aegis Authenticator app from Google Play and install it on my Android phone. Unfortunately, I neither have a google

My IPhone is an old one and can't install "Raivo Authenticator", and then I can't go ahead with the next step. what should I do?

problem?

CERN SSO (slueders)

939 377

#1a: Teach 2FA

I would like to express, though, that the decision to have the 2FA has made
needed
Now, I
otherw
stick.

I use mobile without OS. Unfortunately up to now I have not a smartphone,
use notebook for my work. Need time to purchase a smartphone.

A laptop is almost impossible to forget, but the second, small device will always be absent a few times per month.
CERN has to be aware that, by implementing this policy, the research work will be about 10 to 20% slowlier than before, and that this has consequences on the mental health of the users.

To understand the numbers : if I forget my phone twice in a month, the two full days are almost lost, because I won't come back home only for this - also I have meetings I should follow right in the

For sure you have to sort out the billing of the Yubikeys - is this a HostLab responsibility (in which case the keys should be issued free to users and financed on a central CERN budget, like for access cards) or should users pay? From which account? Has this been discussed in

#1b: Distribute 2FA

Microsoft

Terminal Services

#1c: Fail for 2FA

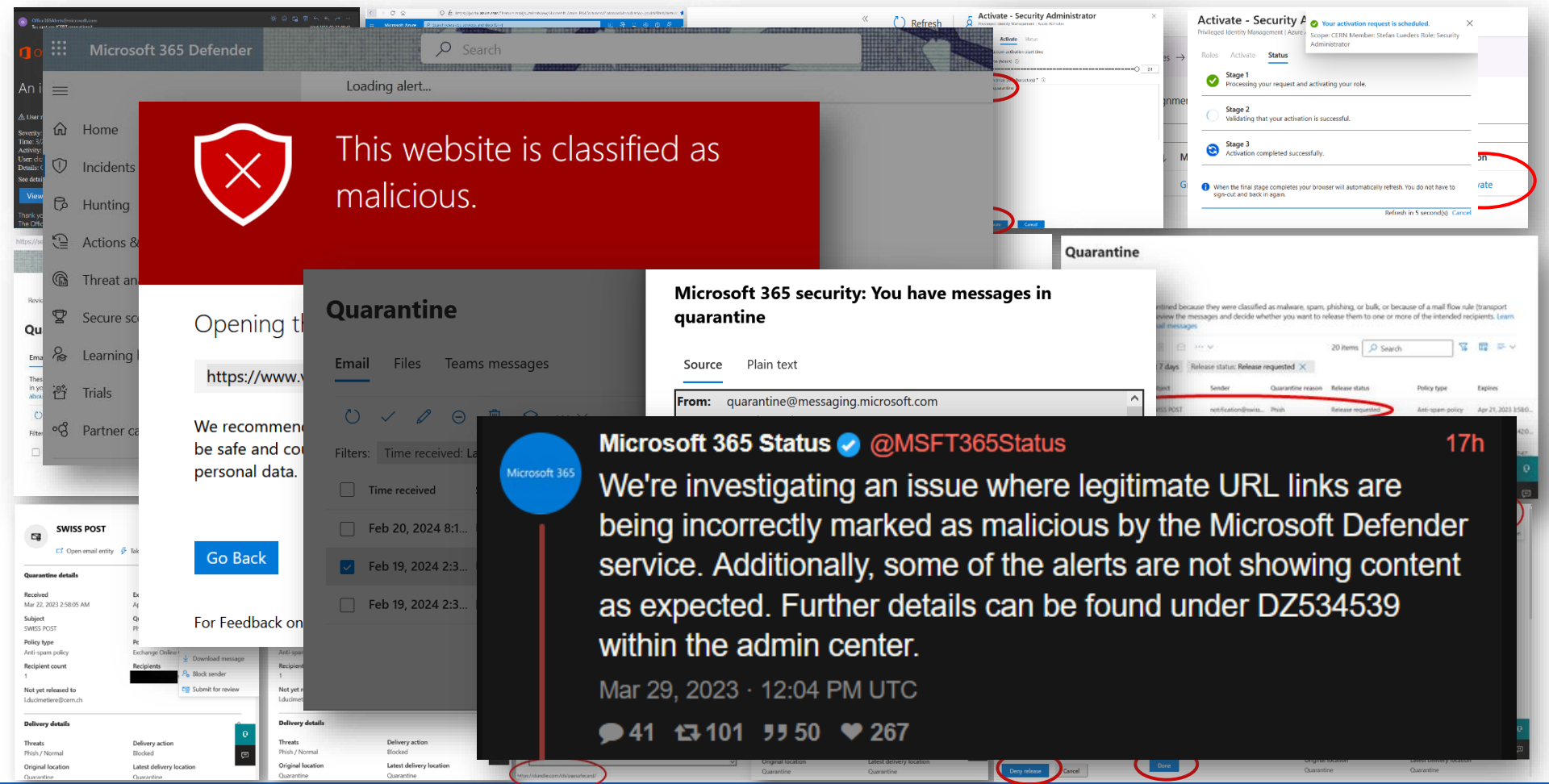
Users send @CERN.ch from Gmail & Co.

Many mailing lists impersonate senders

Many universities wrongly implemented emailing

...and (for legacy reasons) CERN tolerates private emails

#2a: Enforce SPF/DMARC/DKIM



#2b: Rant about quality of cloud services & support

Inform users of exposed passwords

Holding ~1.5B email/password pairs; monitoring ~9k communities;
reporting ~11k exposed passwords per day (~4/day for CERN)

Provide stand-alone EDR

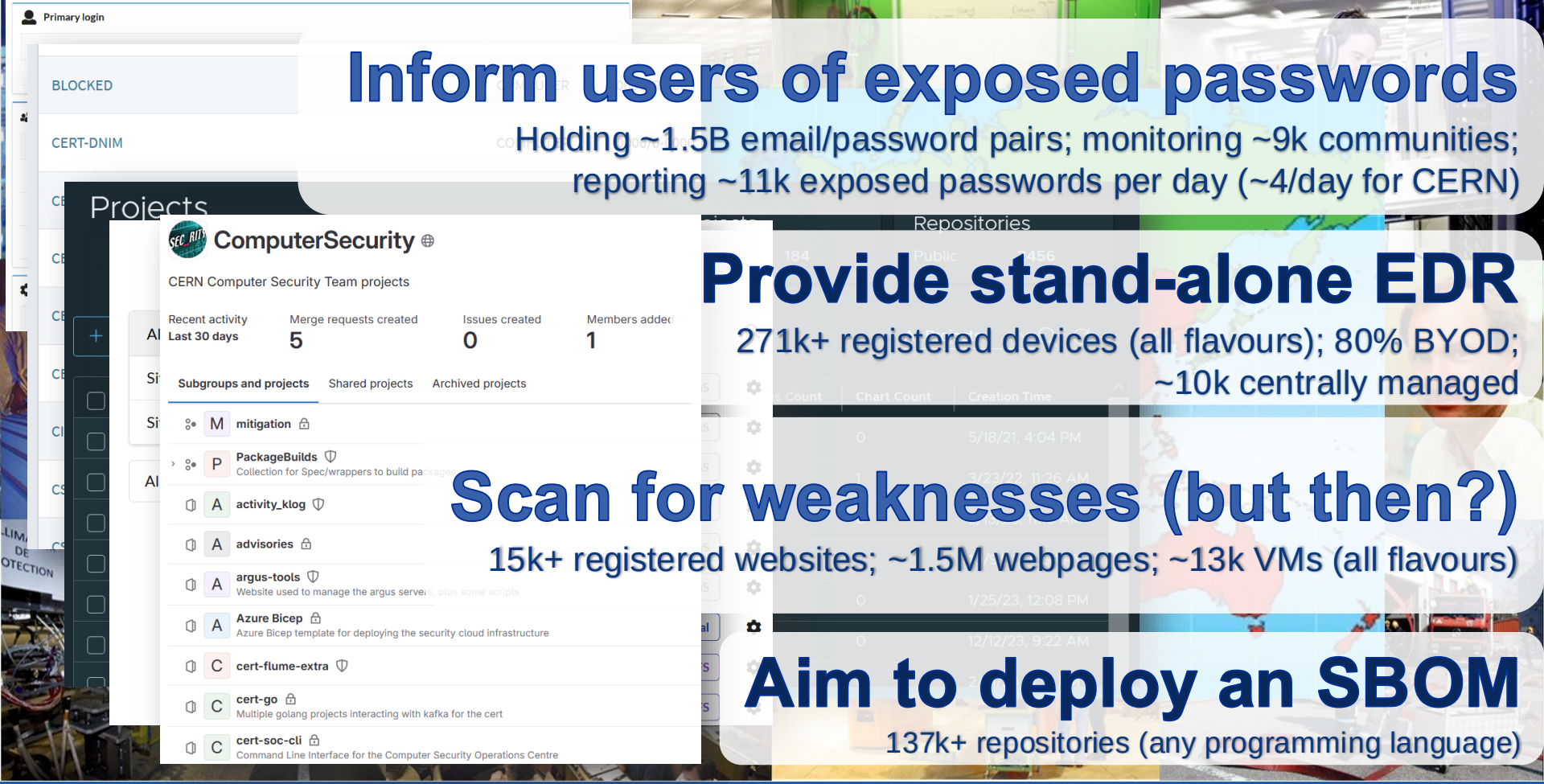
271k+ registered devices (all flavours); 80% BYOD;
~10k centrally managed

Scan for weaknesses (but then?)

15k+ registered websites; ~1.5M webpages; ~13k VMs (all flavours)

Aim to deploy an SBOM

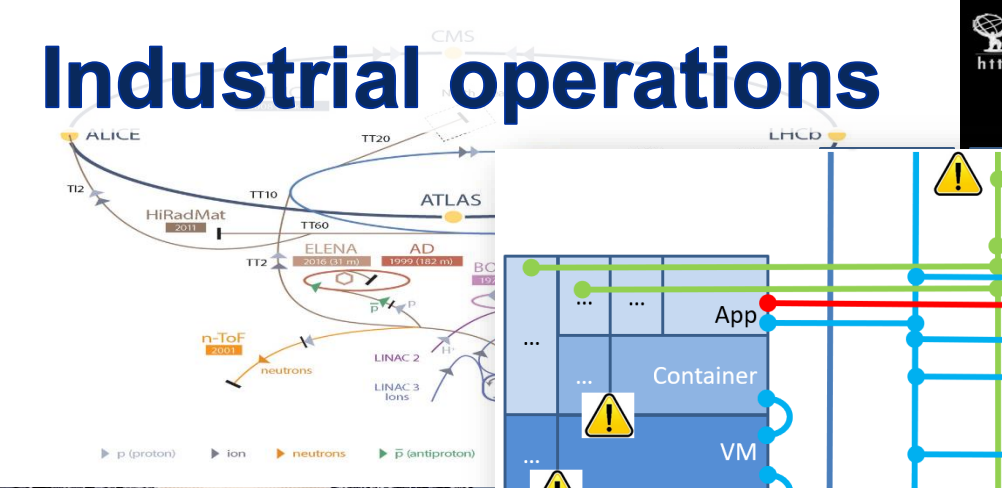
137k+ repositories (any programming language)

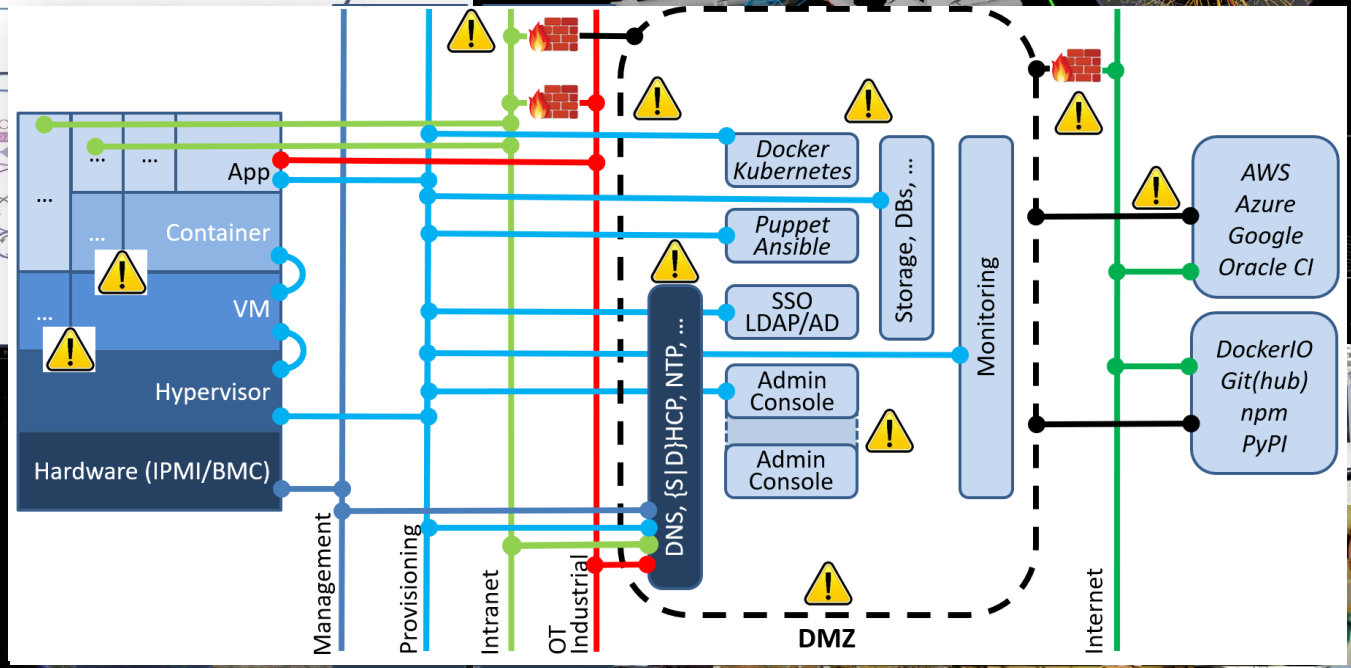


#3a: Assist “Academic Freedom”

Industrial operations

Number crunching

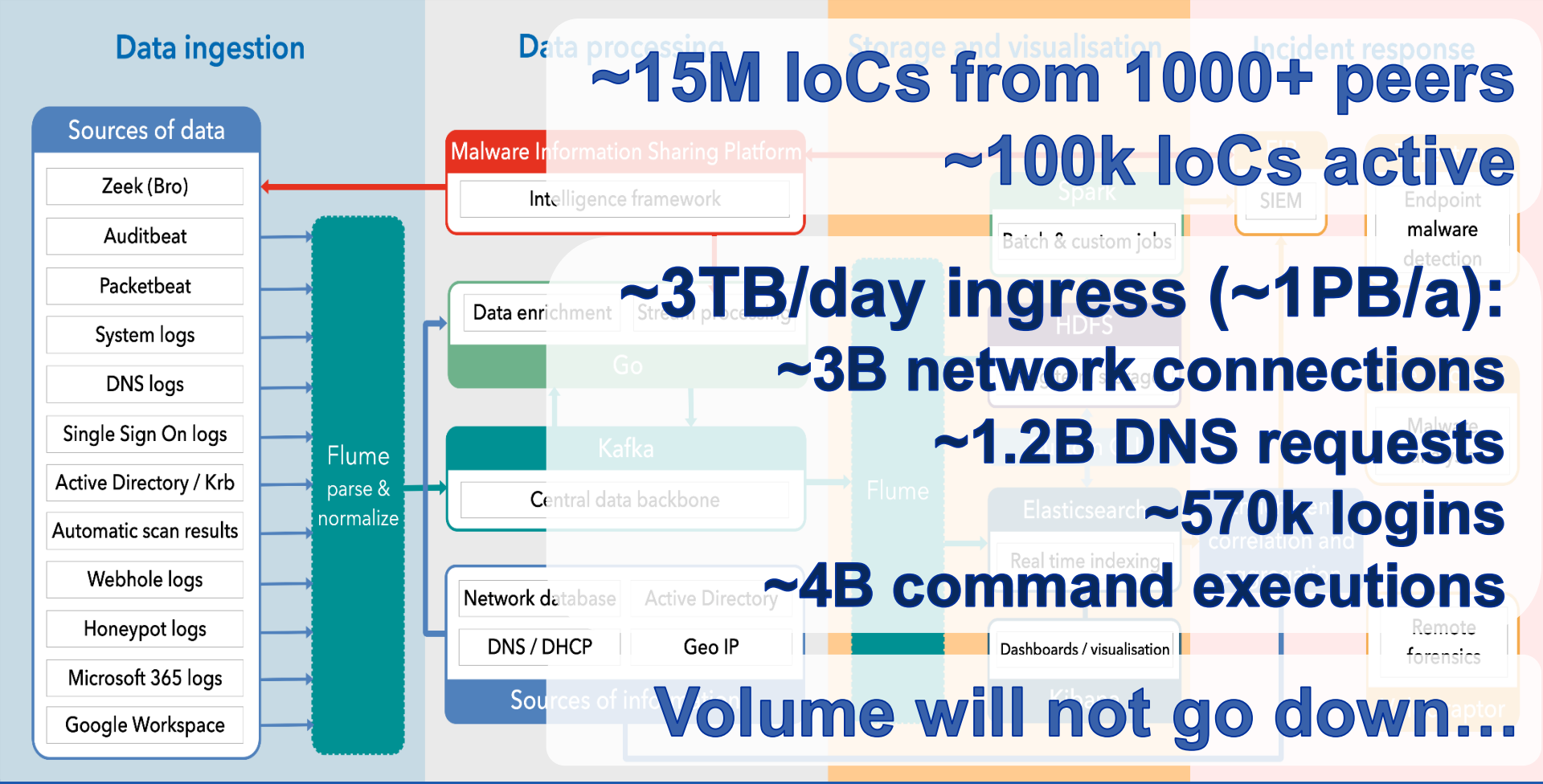




Worldwide cloud

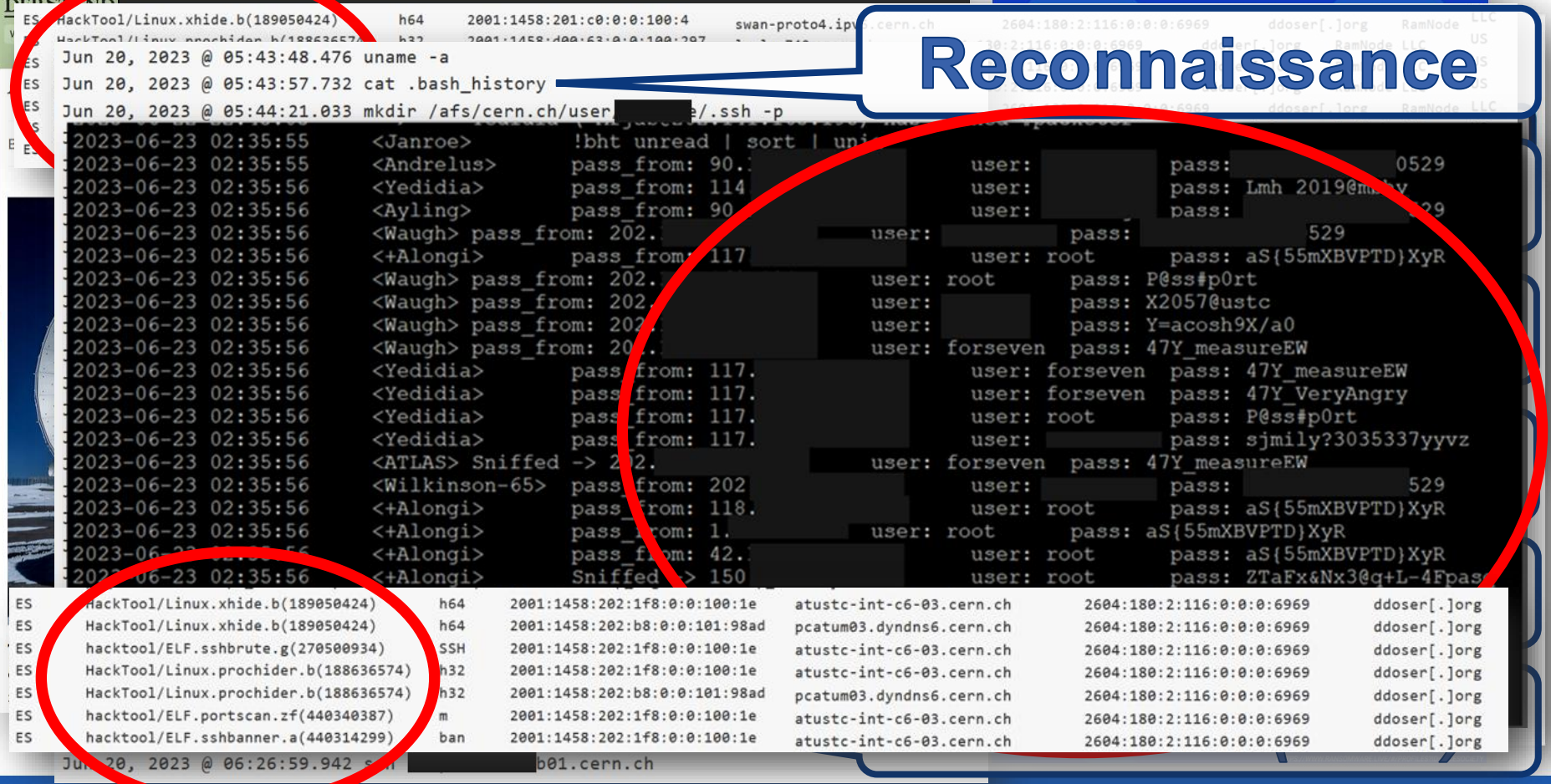
ISP

#3b: Control “Academic Freedom”

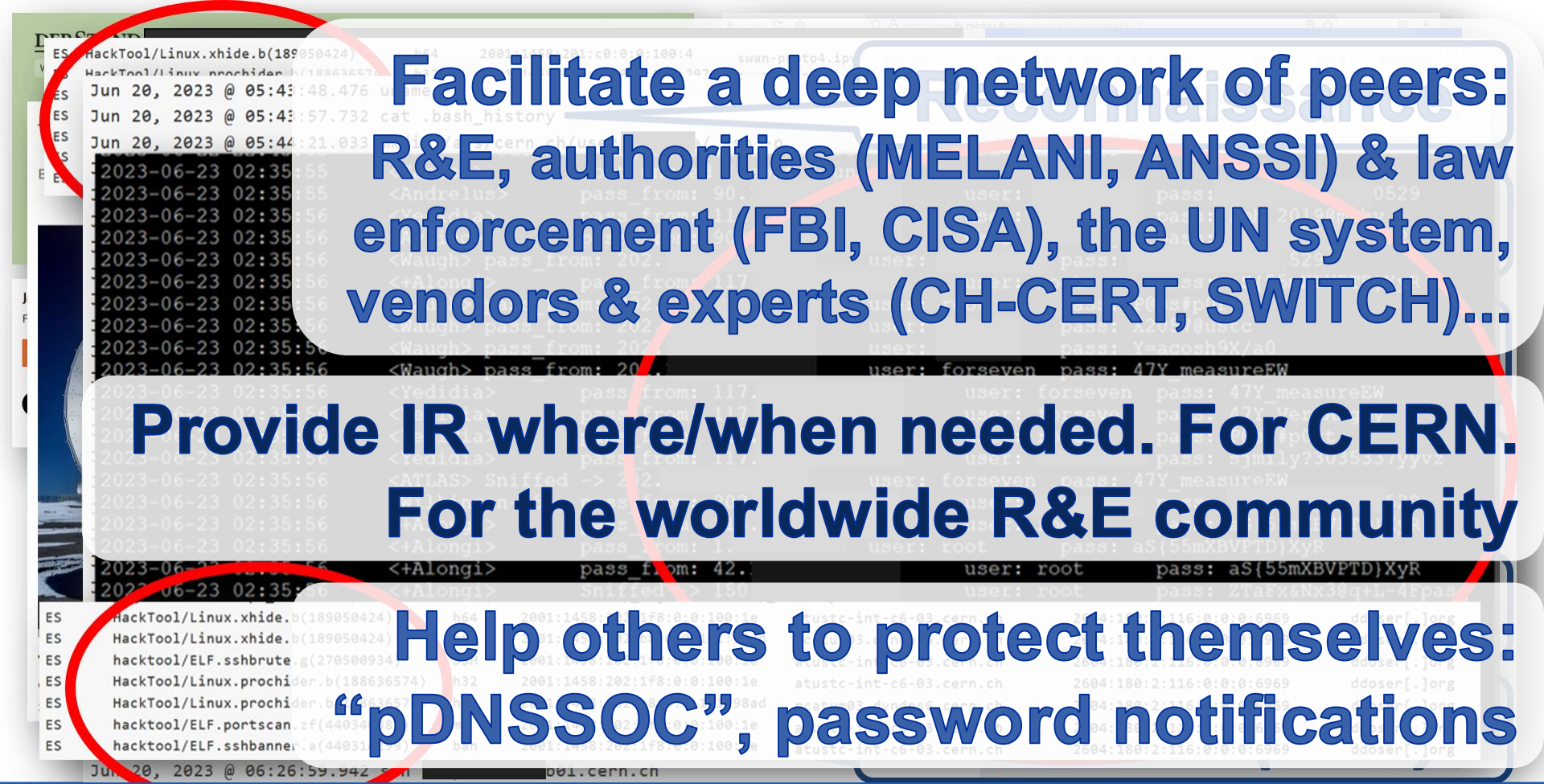


#4: Keep up with Detection

Reconnaissance



R&E has become target... Affirmatively!


Facilitate a deep network of peers:
R&E, authorities (MELANI, ANSSI) & law enforcement (FBI, CISA), the UN system, vendors & experts (CH-CERT, SWITCH)...
Provide IR where/when needed. For CERN. For the worldwide R&E community
Help others to protect themselves: “pDNSSOC”, password notifications

Computer Security Office's Mandate:

Protect CERN's operations & reputation against cyber-threats (incl. the WLCG and our academic R&E community)

Approach: Find a pragmatic balance between "Operations", "Academic Freedom" & "Security"

Strategy:

Enhance CERN's security posture wherever its agility/complexity/heterogeneity allows.

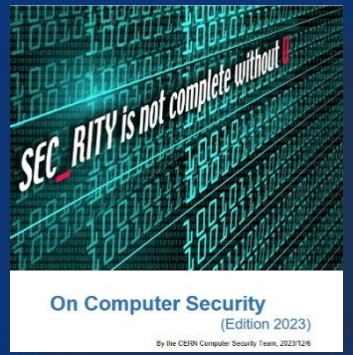
Have excellent threat intel to anticipate attacks.

Defend in depth; detect early; respond quickly & thoroughly

Want to join the challenge?

https://stages.epfl.ch

www.cern.ch



Thank you! Questions?

https://cern.ch/security

https://security.web.cern.ch/training/en/CERN%20Articles%20On%20Computer%20Security.pdf