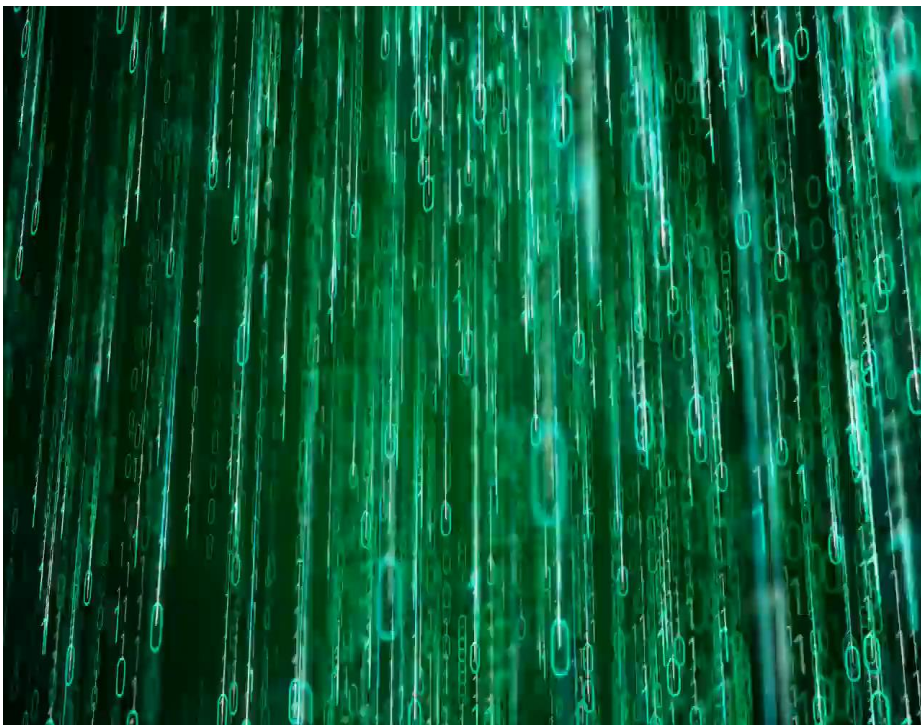


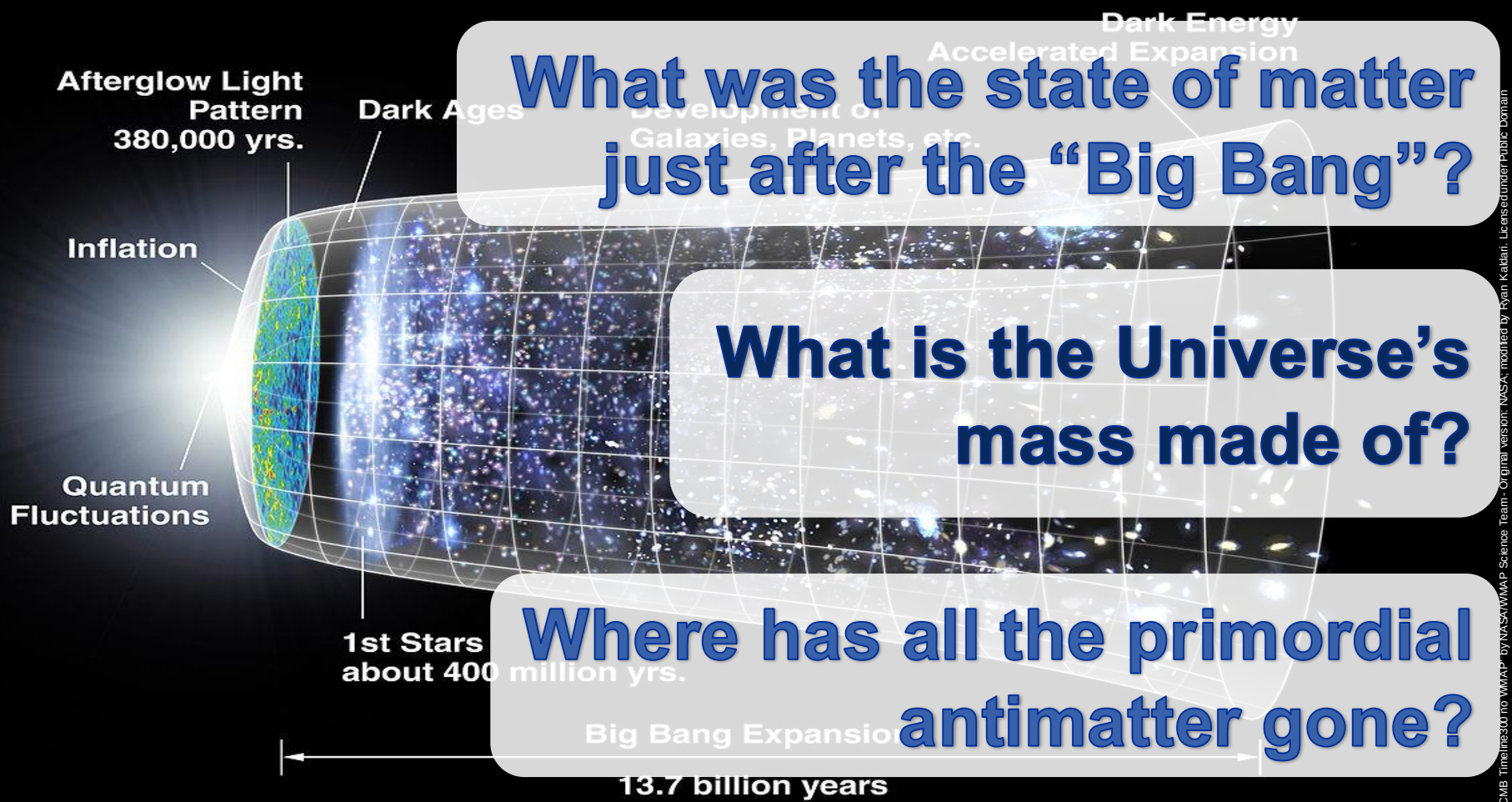


European Organization for Particle Physics
Exploring the frontiers of knowledge



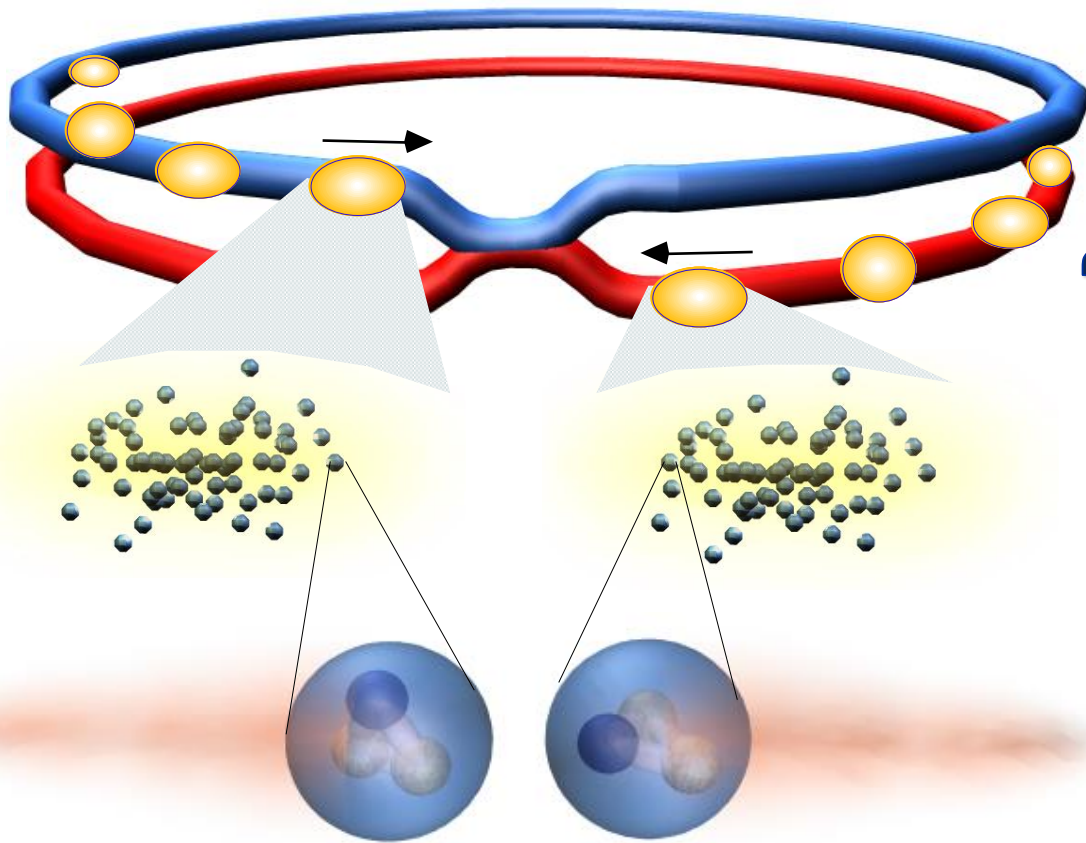
My pick of 5 challenges when protecting Research & Education





CMB Timeline to no WMAP by NASA/WMAP Science Team - Original version: NASA, modified by Ryan Kaldari. License: under Public Domain

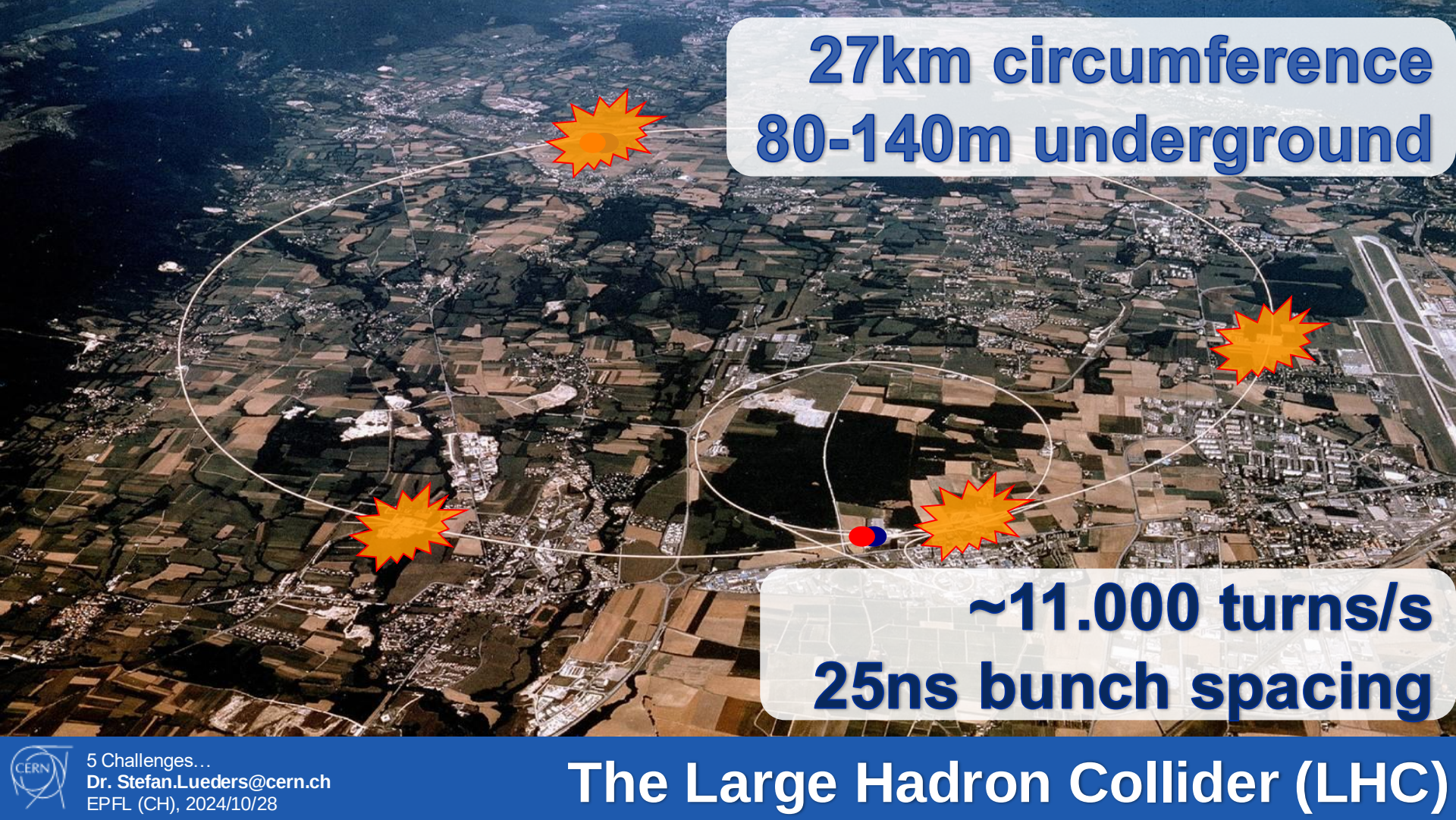




“Beam”: $2 \times 2822b$

“Bunch”: $10^{11}p$

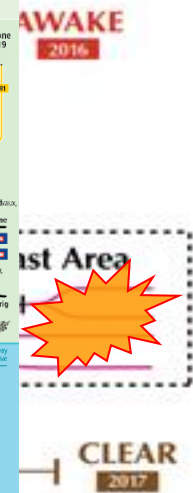
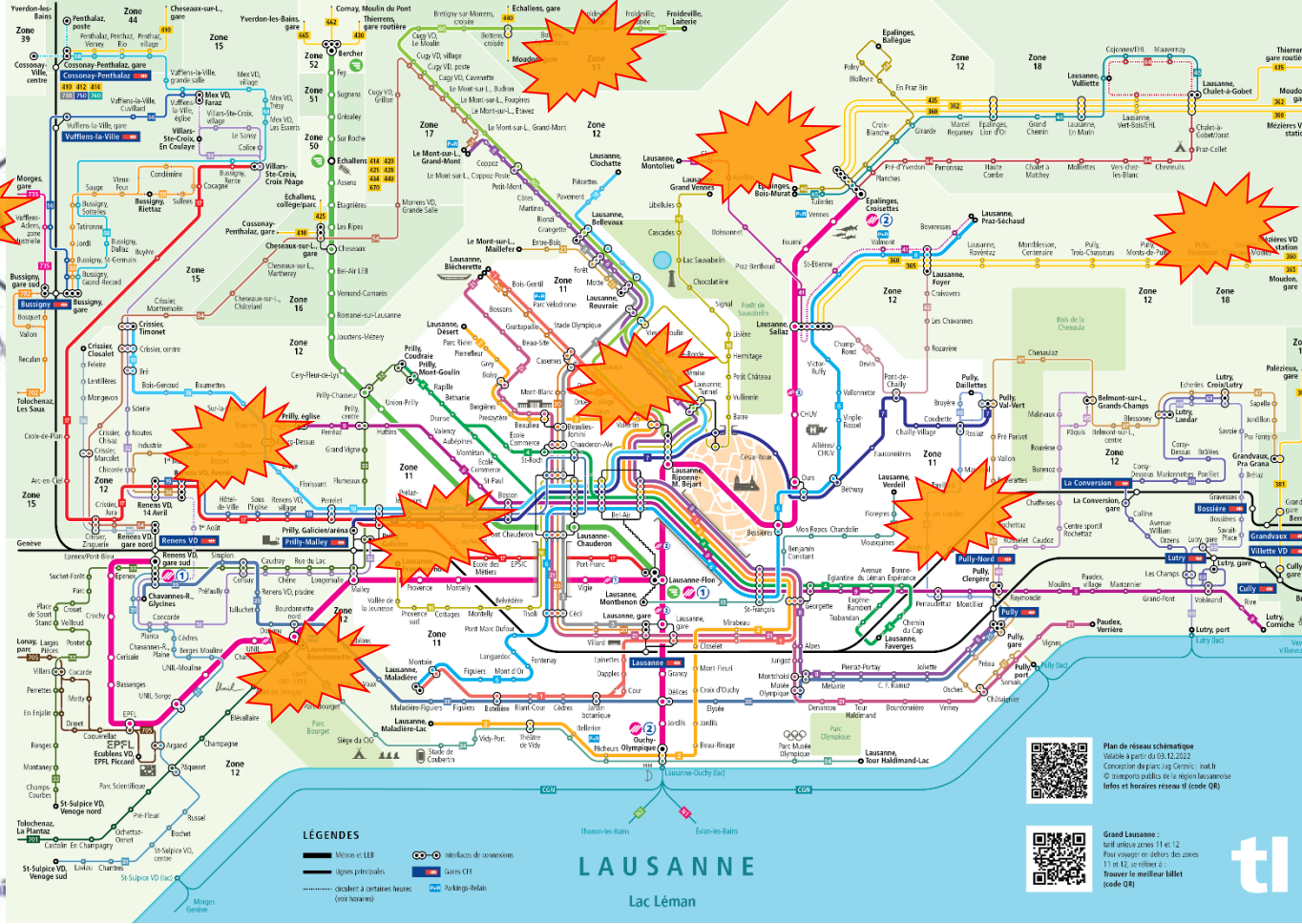
Protons/Quarks



27km circumference
80-140m underground

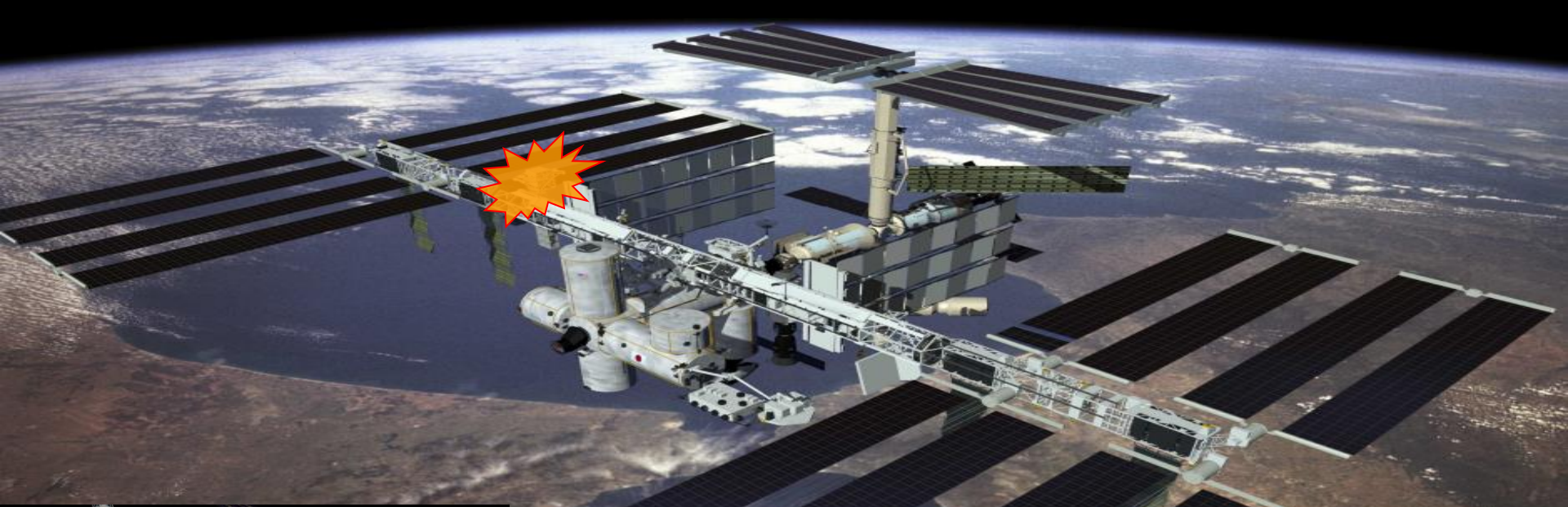
~11.000 turns/s
25ns bunch spacing





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

More than the LHC...



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

...and one detector in space



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

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**

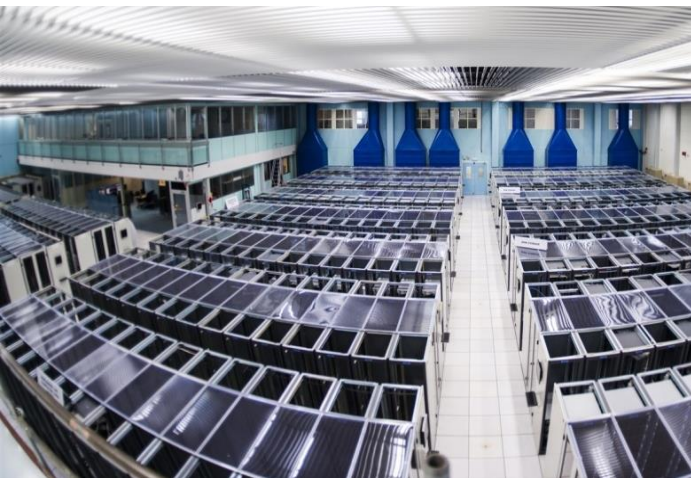
**~271k heterogeneous devices registered:
any hardware, any operating system, any (legal) application**

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



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





~20.000 researchers worldwide



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

CERN's Academic Community

cs1:cs1_login-*

Search field names

Filter by type

Selected fields

_source

Available fields

Popular

method

srcip

success

user

_id

_index

_score

_type

environment

host

hostgroup

pid

srcport

timestamp

tolevel_hostgroup

_type

4 hits

Dec 31, 2022 @ 08:39:30.827 - Jan 30, 2023 @ 08:39:30.827

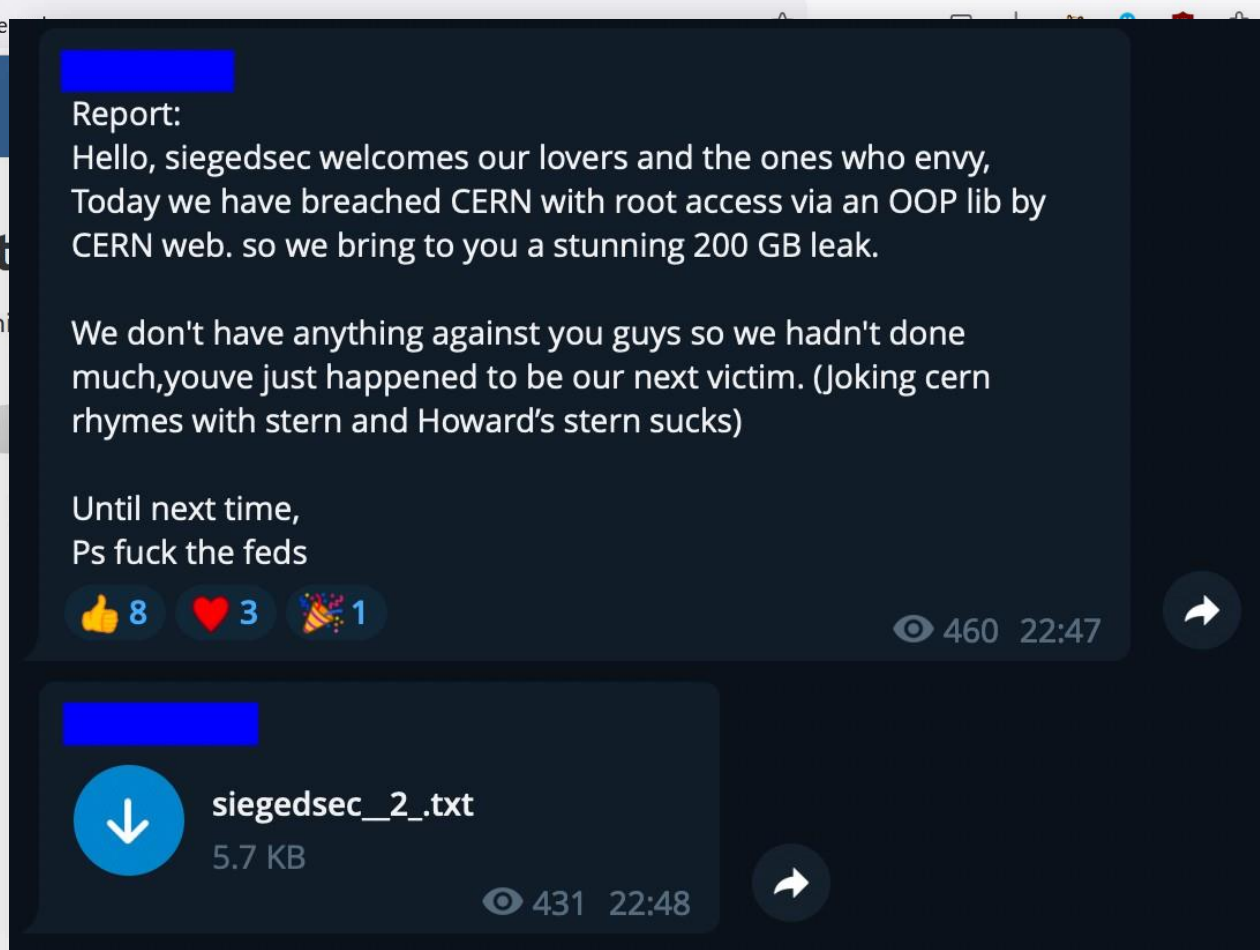
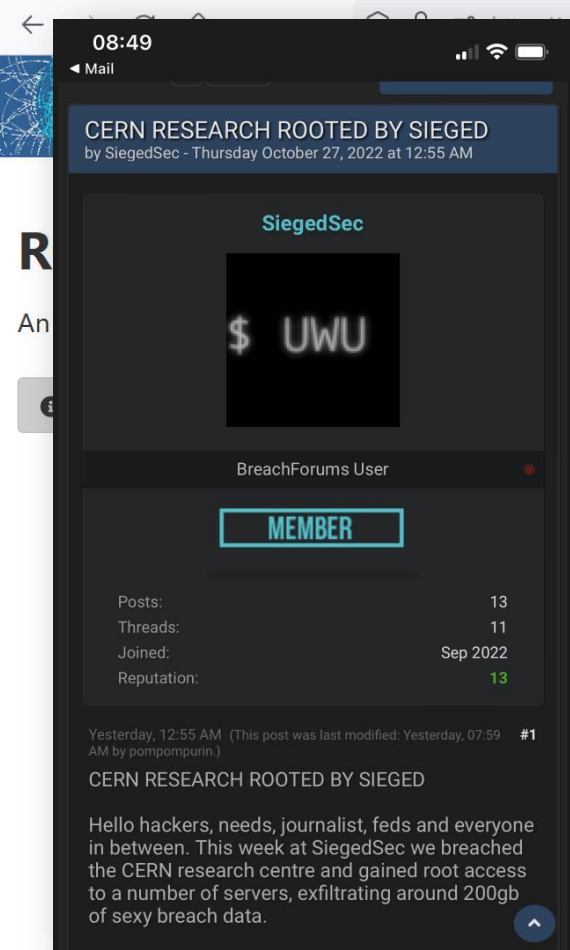
Auto



Time

_source

- > Jan 23, 2023 @ 03:35:36.663 srcip: 194.5.212.214 method: password pid: 1,868,231 type: login toplevel_hostgroup: lxplus environment: qa success: false host: lxplus8s08.cern.ch hostgroup: lxplus/nodes/login srcport: 39,886 user: student6 timestamp: Jan 23, 2023 @ 03:35:36.663 _id: AAABhdx7J1dQA79nzeDc-QmUyFfj5SSZ _type: - _index: cs1:cs1_login-2023.01.23 _score: -
- > Jan 23, 2023 @ 03:12:29.382 srcip: 194.5.212.214 method: password pid: 1,861,287 type: login toplevel_hostgroup: lxplus environment: qa success: false host: lxplus8s08.cern.ch hostgroup: lxplus/nodes/login srcport: 46,308 user: bot timestamp: Jan 23, 2023 @ 03:12:29.382 _id: AAABhdx1-EblCa7ebgo1RkpKIbirYodD _type: - _index: cs1:cs1_login-2023.01.23 _score: -
- > Jan 22, 2023 @ 20:07:43.410 srcip: 194.5.212.214 method: password pid: 640,925 type: login toplevel_hostgroup: lxplus environment: qa success: false host: lxtunnel03.cern.ch hostgroup: lxplus/tunnel srcport: 55,594 user: guest timestamp: Jan 22, 2023 @ 20:07:43.410 _id: AAABhdxGblxA3G377YsIO2562872VC _type: - _index: cs1:cs1_login-2023.01.22 _score: -
- > Jan 22, 2023 @ 19:26:29.650 srcip: 194.5.212.214 method: password pid: 1,605,002 type: login toplevel_hostgroup: lxplus environment: qa success: false host: lxplus8s08.cern.ch hostgroup: lxplus/nodes/login srcport: 58,898 user: timestamp: Jan 22, 2023 @ 19:26:29.650 _id: AAABhdq7WpKwNpm9-K9mIUjryi_F3rky _type: - _index: cs1:cs1_login-2023.01.22 _score: -



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 🙋

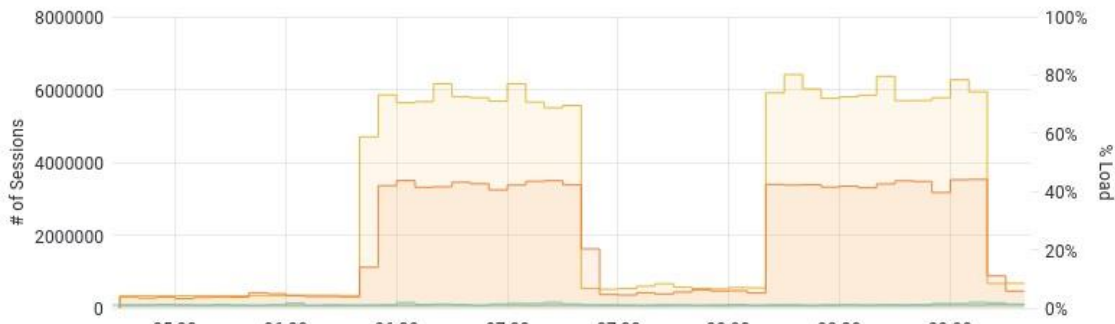
👁 10.3K 18:50

KillMilk

Я так долго ждал этого дня ребята 😭

👁 10.4K 18:51

Sessions and Load - totals



	min	max	avg
GF1P Active Sessions	73998	85747	79380
GF2P Active Sessions	327460	6414111	3033365
GF1P Data Plane load (right-y)	0.700%	1.95%	1.07%
GF2P Data Plane load (right-y)	3.25%	44.2%	23.0%

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



5 Challenges...

Dr. Stefan.Lueders@cern.ch

EPFL (CH), 2024/10/28

DDOSsing CERN (for tests)

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, ...)

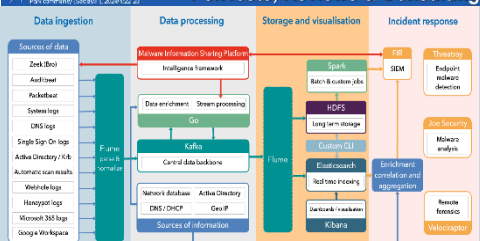
Standard: Audited 2023 against CISv8 (our choice)
82 findings (0 critical, 15 major, 33 moderate, 34 minor); no surprise, all expected;
50% under ODP, 50% under IT department ISTPS
<https://www.cisecurity.org/controls/v8>

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

PenTests, Reviews & Consulting



Orchestration (the "SOC")

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/cern/20Articles%20On%20Computer%20Security.pdf>

Dedicated Training: Providing in-depth training on security practices incl. programming. Plus "Serious Gaming" and "WhiteHat Challenges".
~800 domains blocked by CERN, 100+ by SWITCH. No hospital got ransomware so far
<https://home.cern/news/news/computing/computer-security/when-cernch-not-cern>

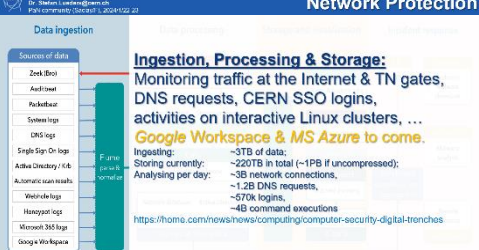
Governance

PaloAlto Firewalling:
Performing deep packet inspection and policy-based IP, domain & URL blocking.
~2x 200Gbps (ingress+egress) IP+4k+6 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+ by SWITCH. No hospital got ransomware so far
<https://home.cern/news/news/computing/computer-security/when-cernch-not-cern>

pDNS Containers: Helping WLCG sites to do alike.

Network Protection



Intrusion Detection

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

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

Dumps of Exposed Passwords:
Notifying when used outside. Ditto for our community. Forcing reset when used at CERN.
Monitoring ~8k communities; reporting ~11k exposed passwords per day (~4day for CERN)
<https://home.cern/news/news/computing/computer-security/passwords-leaked>

Account Protection

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>

Software Security



Incident Response

EOP - xorlab - MDO eMail-Filtering:
Quarantining SPAM & malware.
~115k analyzed per day; 10% SPAM; 2% quarantined; 1/20 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-on-free-pipe-your-device>

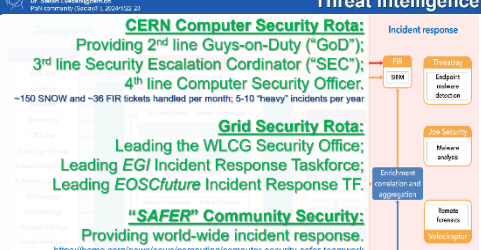
Threat Memory Hashing:
Detecting anomalies on CERN-managed devices.
~5500 CERN-managed devices enrolled

Endpoint Protection

ThreatIntel: Obtaining high-quality indicators of compromise.
~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.
Pex: 120+ universities world-wide notified this year of ransomware preparations in their IT infrastructure

Threat Intelligence



CERN & HEP CSIRT



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

A Comprehensive Porte-Folio



SECURITY

is not complete without

U

5 challenges when protecting Research & Education



5 Challenges...

Dr. Stefan.Lueders@cern.ch

EPFL (CH), 2024/10/28

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 I've got a lot of problems

sel

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

How to
screen
should
proced

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 or
then I can't go ahead with the next step. what should I do?
problem?

CERN SSO (slueders)

939 377



ente



I would like to express though, that the decision to have the 2FA has made I need 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% slower 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





Microsoft

Terminal Services



Microsoft Defender
for Office 365



xorlab

The move means that DMARC, already in use by half of enterprises, will become a must for anyone using email for marketing.

The requirements — announced by Google and Yahoo this week — will reach much more than marketers, however, forcing all companies lagging behind in their adoption of the trio of security technologies to catch up. Email authentication standards such as DomainKeys Identified Mail (DKIM) will gain protection against impersonation through better authentication, while DMARC creates a notification channel for domain owners to collect information on whether their email is being spoofed.

**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



Microsoft 365 Defender

Loading alert...

This website is classified as malicious.

Quarantine

Opening the message...

https://www.v...

We recommend you be safe and complete your personal data.

Go Back

For Feedback on...

Microsoft 365 security: You have messages in quarantine

Source Plain text

From: quarantine@messaging.microsoft.com

Microsoft 365 Status @MSFT365Status 17h

We're investigating an issue where legitimate URL links are being incorrectly marked as malicious by the Microsoft Defender service. Additionally, some of the alerts are not showing content as expected. Further details can be found under DZ534539 within the admin center.

Mar 29, 2023 · 12:04 PM UTC

41 101 50 267

https://handson.azurewebsites.net/

Only release Cancel Done

Activate - Security Administrator

Privileged Identity Management (Azure)

Scopes: CERN Member: Stefan Lueders Role: Security Administrator

Roles Activate Status

Stage 1 Processing your request and activating your role.

Stage 2 Validating that your activation is successful.

Stage 3 Activation completed successfully.

When the final stage completes your browser will automatically refresh. You do not have to sign-out and back in again.

Refresh in 5 seconds Cancel

Quarantine

20 items Search

7 days Release status: Release requested X

7 days POST notification@cern.ch Phish Release requested Anti-spam policy Apr 21, 2023 15:00...

Quarantine details

Received Mar 22, 2023 2:58:05 AM

Subject SWISS POST

Policy type Anti-spam policy

Recipient count 1

Not yet released to lducometiere@cern.ch

Delivery details

Threats Phish / Normal

Original location Quarantine

Latest delivery location Quarantine

Delivery action Blocked

Latest delivery location Quarantine



BLOCKED

CERT-DNIM

Projects

**ComputerSecurity**

CERN Computer Security Team projects

Recent activity
Last 30 daysMerge requests created
5Issues created
0Members added
1

Subgroups and projects

Shared projects

Archived projects

M mitigation

P PackageBuilds
Collection for Spec/wrappers to build packages

A activity_klog

A advisories

A argus-tools
Website used to manage the argus servers, plus some scriptsA Azure Bicep
Azure Bicep template for deploying the security cloud infrastructure

C cert-flume-extra

C cert-go
Multiple golang projects interacting with kafka for the certC cert-soc-cli
Command Line Interface for the Computer Security Operations Centre

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)

5 Challenges...

Dr. Stefan.Lueders@cern.ch

EPFL (CH), 2024/10/28

#3a: Assist “Academic Freedom”

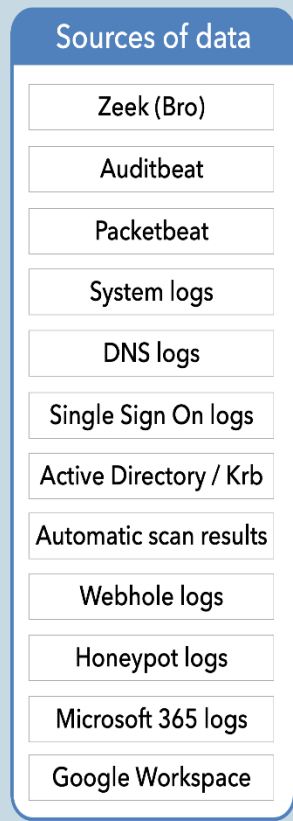
ATLAS
EXPERIMENT
<http://atlas.cern.ch>

ATLAS
EXPERIMENT
<http://atlas.cern.ch>



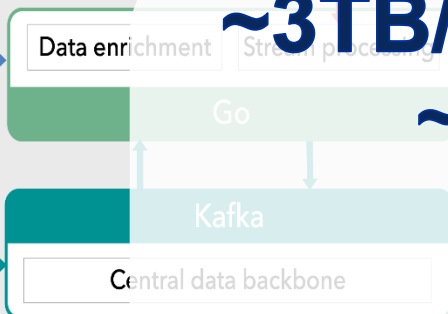
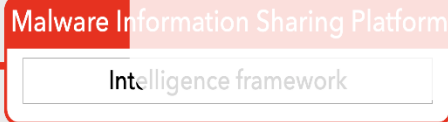
Worldwide cloud

Data ingestion



Flume
parse &
normalize

Data processing



Sources of information

Storage and visualisation



Incident response

~15M IoCs from 1000+ peers

~100k IoCs active

~3TB/day ingress (~1PB/a):

~3B network connections

~1.2B DNS requests

~570k logins

~4B command executions

Volume will not go down...



Reconnaissance

```
Jun 20, 2023 @ 05:43:48.476 uname -a
```

```
Jun 20, 2023 @ 05:43:57.732 cat .bash_history
```

```
Jun 20, 2023 @ 05:44:21.033 mkdir /afs/cern.ch/user/.../ssh -p
```

```
2023-06-23 02:35:55 <Janroe> !bht unread | sort | uni
2023-06-23 02:35:55 <Andrelus> pass_from: 90. user: pass: 0529
2023-06-23 02:35:56 <Yedidia> pass_from: 114 user: pass: Lmh 2019@...
2023-06-23 02:35:56 <Ayling> pass_from: 90 user: pass: 29
2023-06-23 02:35:56 <Waugh> pass_from: 202. user: pass: 529
2023-06-23 02:35:56 <+Alongi> pass_from: 117 user: root pass: aS{55mXBVPTD}XyR
2023-06-23 02:35:56 <Waugh> pass_from: 202. user: root pass: P@ss#p0rt
2023-06-23 02:35:56 <Waugh> pass_from: 202. user: pass: X2057@ustc
2023-06-23 02:35:56 <Waugh> pass_from: 202. user: pass: Y=acosh9X/a0
2023-06-23 02:35:56 <Waugh> pass_from: 202. user: forseven pass: 47Y_measureEW
2023-06-23 02:35:56 <Yedidia> pass_from: 117. user: forseven pass: 47Y_measureEW
2023-06-23 02:35:56 <Yedidia> pass_from: 117. user: forseven pass: 47Y_VeryAngry
2023-06-23 02:35:56 <Yedidia> pass_from: 117. user: root pass: P@ss#p0rt
2023-06-23 02:35:56 <Yedidia> pass_from: 117. user: pass: sjmily?3035337yyvz
2023-06-23 02:35:56 <ATLAS> Sniffed -> 202. user: forseven pass: 47Y_measureEW
2023-06-23 02:35:56 <Wilkinson-65> pass_from: 202. user: pass: 529
2023-06-23 02:35:56 <+Alongi> pass_from: 118. user: root pass: aS{55mXBVPTD}XyR
2023-06-23 02:35:56 <+Alongi> pass_from: 1. user: root pass: aS{55mXBVPTD}XyR
2023-06-23 02:35:56 <+Alongi> pass_from: 42. user: root pass: aS{55mXBVPTD}XyR
2023-06-23 02:35:56 <+Alongi> Sniffed -> 150 user: root pass: ZTaFx&Nx3@q+L-4Fpas
```

ES	HackTool/Linux.xhide.b(189050424)	h64	2001:1458:202:1f8:0:0:100:1e	atustc-int-c6-03.cern.ch	2604:180:2:116:0:0:0:6969	ddos[.]org
ES	HackTool/Linux.xhide.b(189050424)	h64	2001:1458:202:b8:0:0:101:98ad	pcatum03.dyndns6.cern.ch	2604:180:2:116:0:0:0:6969	ddos[.]org
ES	hacktool/ELF.sshbrute.g(270500934)	SSH	2001:1458:202:1f8:0:0:100:1e	atustc-int-c6-03.cern.ch	2604:180:2:116:0:0:0:6969	ddos[.]org
ES	HackTool/Linux.prochider.b(188636574)	h32	2001:1458:202:1f8:0:0:100:1e	atustc-int-c6-03.cern.ch	2604:180:2:116:0:0:0:6969	ddos[.]org
ES	HackTool/Linux.prochider.b(188636574)	h32	2001:1458:202:b8:0:0:101:98ad	pcatum03.dyndns6.cern.ch	2604:180:2:116:0:0:0:6969	ddos[.]org
ES	hacktool/ELF.portscan.zf(440340387)	m	2001:1458:202:1f8:0:0:100:1e	atustc-int-c6-03.cern.ch	2604:180:2:116:0:0:0:6969	ddos[.]org
ES	hacktool/ELF.sshbanner.a(440314299)	ban	2001:1458:202:1f8:0:0:100:1e	atustc-int-c6-03.cern.ch	2604:180:2:116:0:0:0:6969	ddos[.]org

```
Jun 20, 2023 @ 06:26:59.942 ssh 2001:1458:202:1f8:0:0:100:1e
```

**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>

