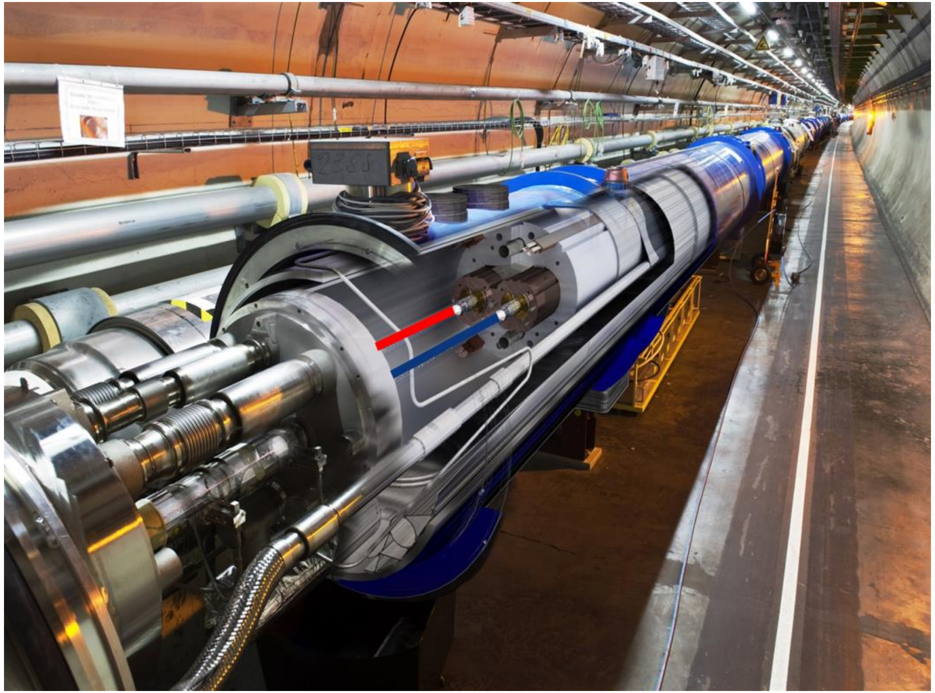
CERN

European Organization for Particle Physics

Exploring the frontiers of knowledge

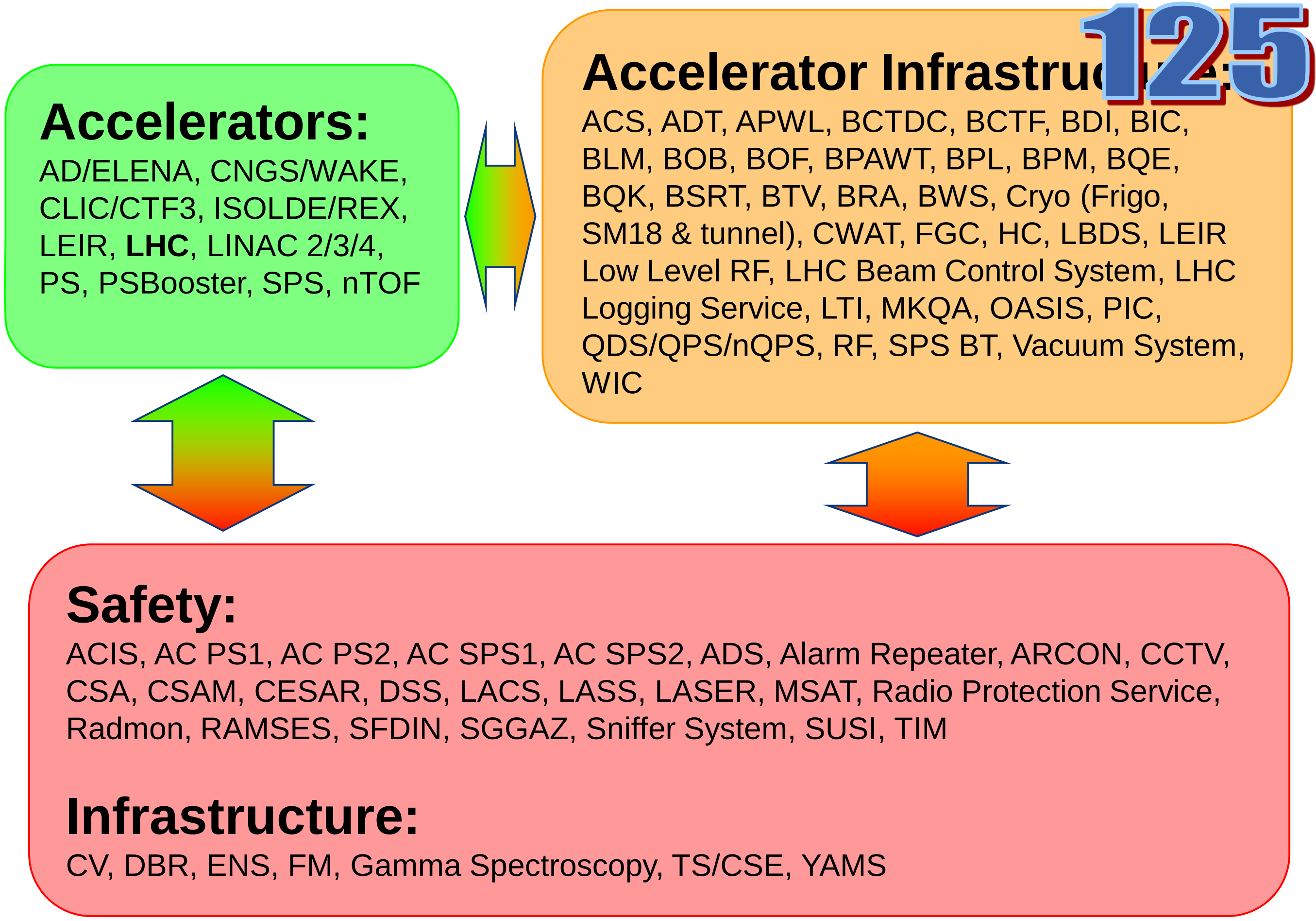


5 Challenges to Secure the LHC...

...and how we (failed to) over come them

5th Control System Cyber-Security Workshop
Dr. Stefan.Lueders@cern.ch
October 18th 2015, Melbourne (AUS)

125+ ICSes



Accelerators:

AD/ELENA, CNGS/WAKE, CLIC/CTF3, ISOLDE/REX, LEIR, **LHC**, LINAC 2/3/4, PS, PSBooster, SPS, nTOF

Accelerator Infrastructure:

ACS, ADT, APWL, BCTDC, BCTF, BDI, BIC, BLM, BOB, BOF, BPAWT, BPL, BPM, BQE, BQK, BSRT, BTV, BRA, BWS, Cryo (Frigo, SM18 & tunnel), CWAT, FGC, HC, LBDS, LEIR Low Level RF, LHC Beam Control System, LHC Logging Service, LTI, MKQA, OASIS, PIC, QDS/QPS/nQPS, RF, SPS BT, Vacuum System, WIC

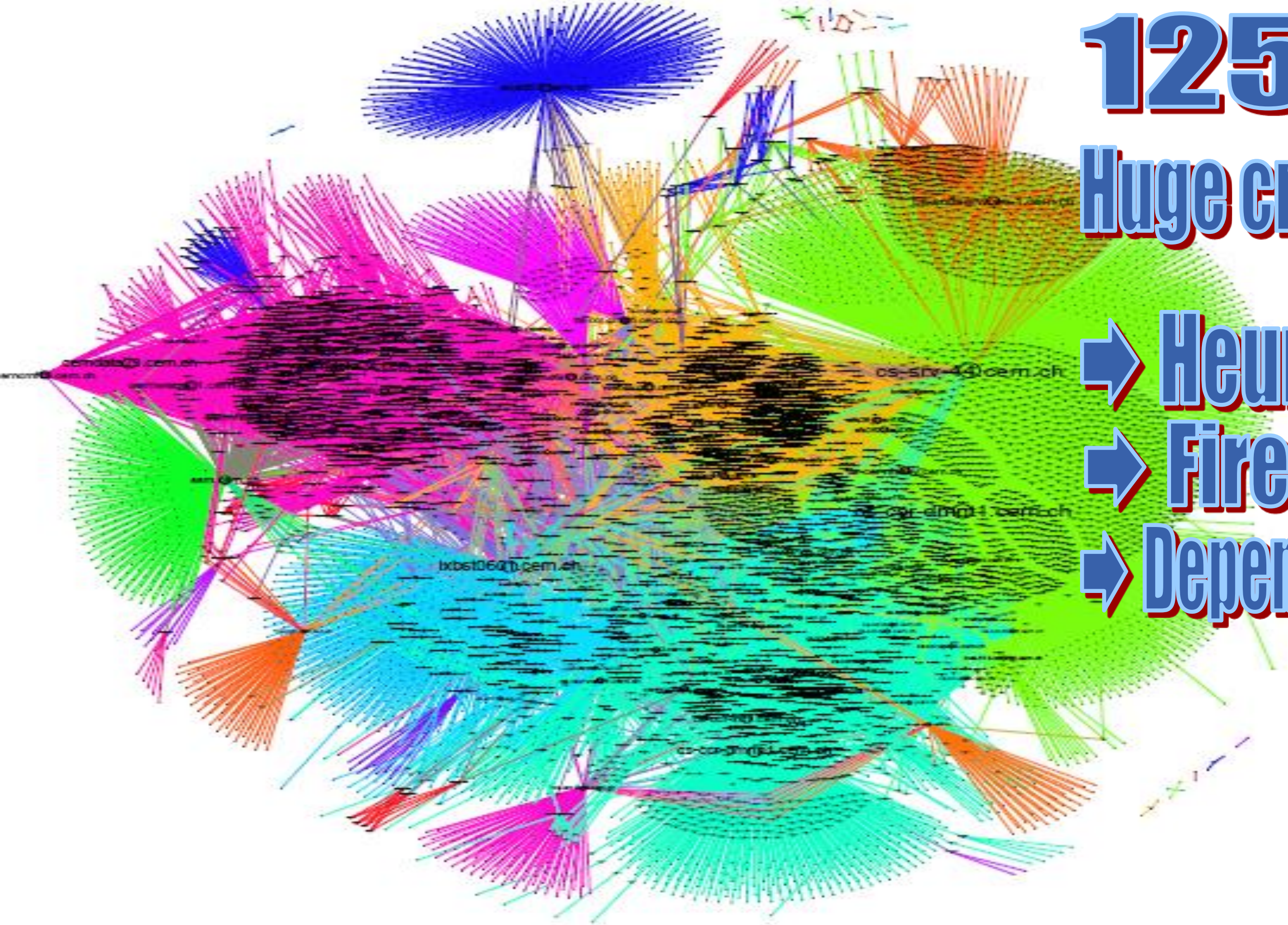
Safety:

ACIS, AC PS1, AC PS2, AC SPS1, AC SPS2, ADS, Alarm Repeater, ARCON, CCTV, CSA, CSAM, CESAR, DSS, LACS, LASS, LASER, MSAT, Radio Protection Service, Radmon, RAMSES, SFDIN, SGGAZ, Sniffer System, SUSI, TIM

Infrastructure:

CV, DBR, ENS, FM, Gamma Spectroscopy, TS/CSE, YAMS

Heterogeneous Cacophony



125+ ICSes

Huge cross-dependencies

- ➡ Heuristic IDS difficult
- ➡ Firewalling complex
- ➡ Dependencies impede APTs

Heterogeneous Cacophony

125+ ICSes

Huge cross-dependencies

➔ Heuristic IDS difficult

➔ Firewalling complex

➔ Dependencies impede APTs

Part of DC acting as DMZ

➔ Regular disco tests

Heterogeneous Cacophony

Few test-stands
400+ developpers

One-Time Prototype

SPB
GNI
Nova
Revit
INDICO
Flume
Java
HDL
Nios
PHP
ExtJS
Altera
Motion
Debian
Saber
C/C++
Maya
JIRA
PCI
Inventor
YUI
Corba
STEP7OA
Jenkins
OPERA
EditPlus
Bamboo
ModelSim
ProVision
Allegro
Modernizr
LeCroy
Drupal
AsciiDoc
Windows 2000
Lightbox
Synplify
Windows 8
AngularJS
DWG
Netviewer
Tektronix
MAX+PLUS
Ansys
MySQL
Showcase
WinCC OA
TPA
Codesys
Wordpress
OpenStack
VISUAL-ELITE
Automotive
Roger
Apache
jQuery
TimingDesigner
Ruby
Web2py
WaveFormer
Erlang
Lo-dash
MicroWave
PCIe-XpressLite
Ceph
Windows XP
Softimage
Mathcad
Siemens TIA Portal
OSGi
ElasticSearch
DFS
CodeIgniter
Tr-Ciel
PAC-Designer
Microwave
SketchBook
ISE
Prototype
Flux
Sonatype Nexus
PSpice
Laravel
Dokuwiki
RabbitMQ
Sharepoint
IIS
Scala
Express
Windows 2003
Vidyo
ispLEVER
CherryPy
SIMPLORER
Windows 98
OracleDB
ServiceNow
AutoCAD
Teamviewer
Pure CSS
XRegExp
AutoVue
PCI-X
ASP.NET
Atlassian
Mechanical
React
Ubuntu
Mudbox
gitlab
Maxwell
MacOS
Tomcat
RedHat
Quartus
MATLAB
Joomla
Libero
Ansoft
Lync
Trace
Glance
Suse
JTAG
Altium
NFS
EDK
VMware
Apex
CATIA
Dojo
PCB
Perl
REST
Code

Few test-stands

400+ developpers

→ Permanent optimizations

→ Agile developpment

~~Windows Terminal Services~~, now ~400 VMs

→ Plans to move dev. out

→ Need choke points

One-Time Prototype

24h/7d/~300d

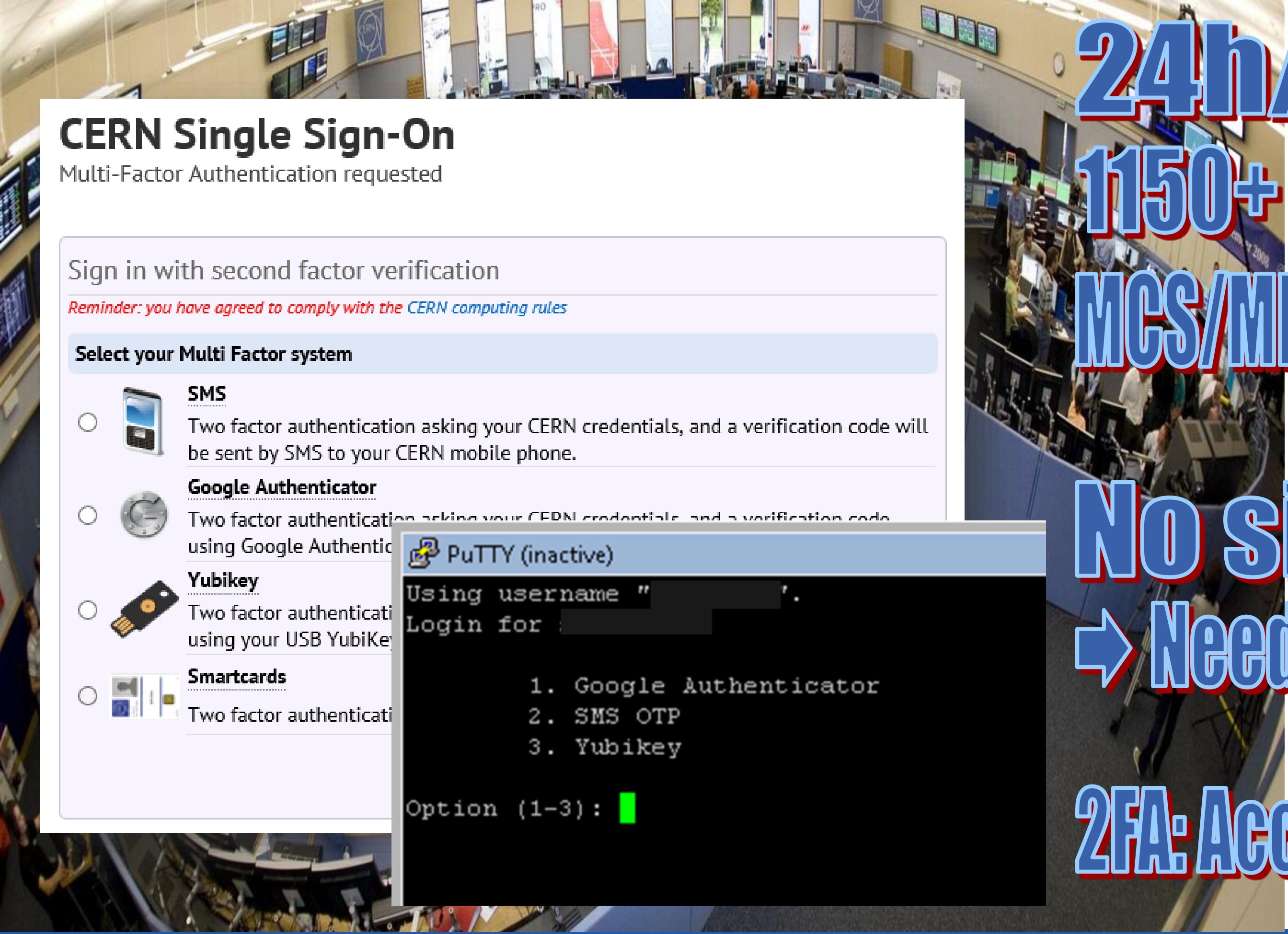
1150+ remote experts

MCS/MPS to avoid blunder

No silver bullet

→ Need proper gateways

Permanent Remote Access



CERN Single Sign-On

Multi-Factor Authentication requested

Sign in with second factor verification

Reminder: you have agreed to comply with the CERN computing rules

Select your Multi Factor system

○ **SMS**
Two factor authentication asking your CERN credentials, and a verification code will be sent by SMS to your CERN mobile phone.

○ **Google Authenticator**
Two factor authentication asking your CERN credentials, and a verification code using Google Authentic

○ **Yubikey**
Two factor authenticati using your USB YubiKe

○ **Smartcards**
Two factor authenticati

PuTTY (inactive)

```
Using username "[redacted]".
Login for [redacted]

        1. Google Authenticator
        2. SMS OTP
        3. Yubikey

Option (1-3): 
```

24h/7d/~300d

1150+ remote experts

MCS/MPS to avoid blunder

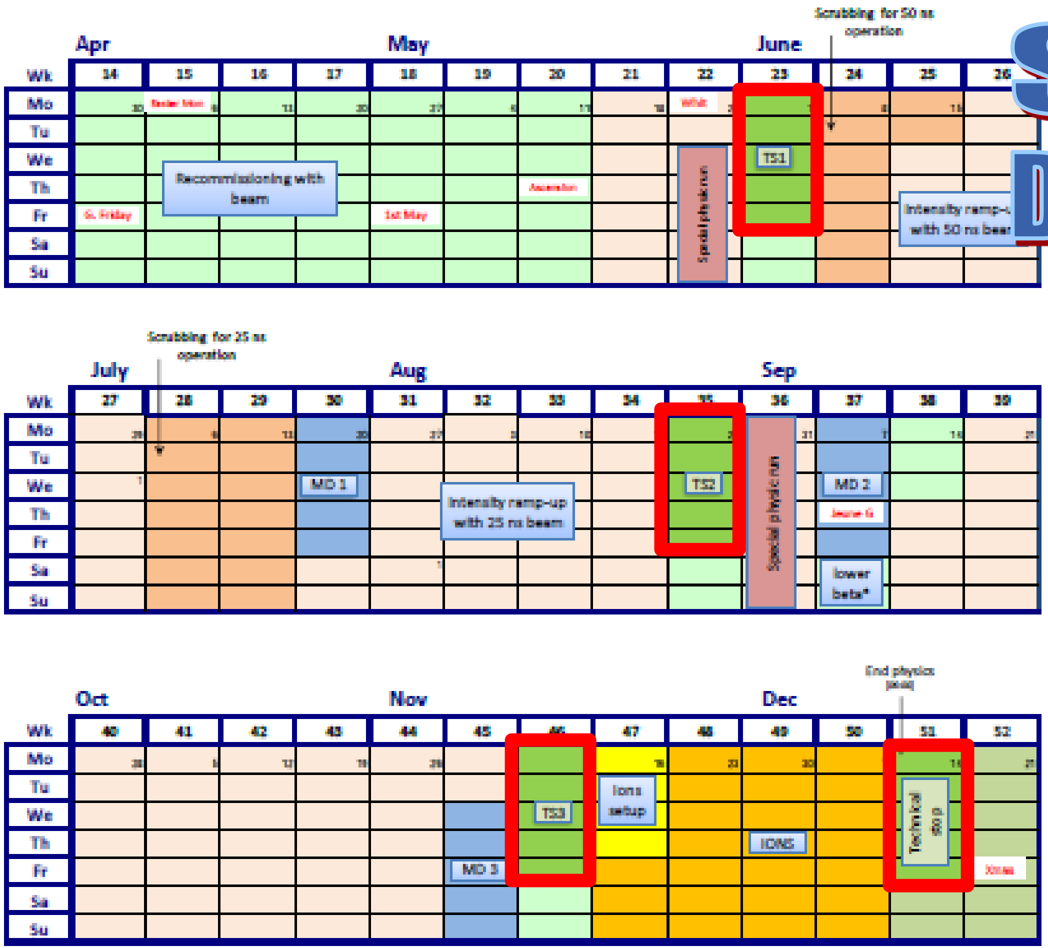
No silver bullet

➔ Need proper gateways

2FA: Acceptance threshold

Permanent Remote Access

Stops rare
DC essential, then



Scrubbing for 50 ns operation

Wk	14	15	16	17	18	19	20	21	22	23	24	25	26
	Apr				May					June			
Mo	30	Easter Mon 6	13	20	27	4	11	18	Whit 25	1	8	15	
Tu													
We		Recommissioning with beam							Special physics run	TS1			
Th							Ascension						
Fr	G. Friday				1st May							Intensity ramp-u with 50 ns bear	
Sa													
Su													

Scrubbing for 25 ns operation

Wk	27	28	29	30	31	32	33	34	35	36	37	38	39
	July				Aug					Sep			
Mo	29	6	13	20	27	3	10		24	31	7	14	21
Tu													
We	1			MD 1					TS2	Special physics run	MD 2		
Th						Intensity ramp-up with 25 ns beam					Jeune G		
Fr													
Sa					1						lower beta*		
Su													

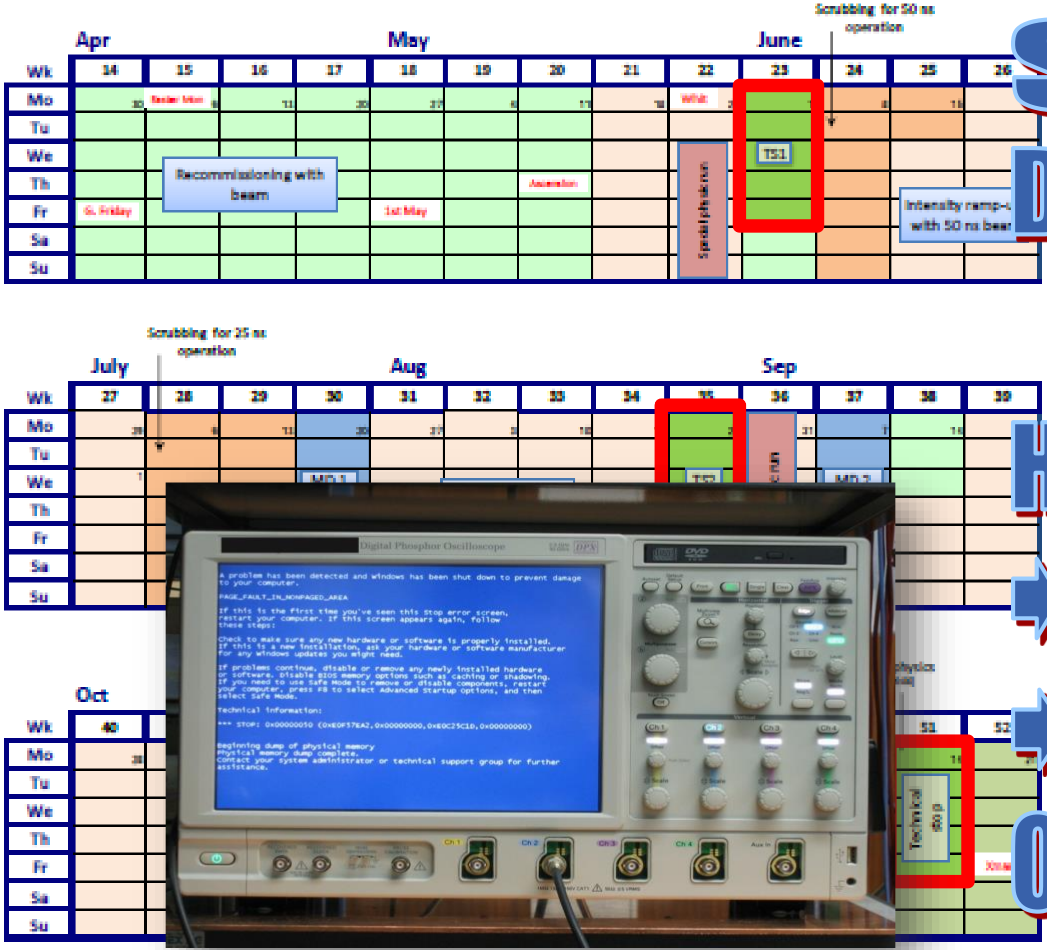
End physics (pp)

Wk	40	41	42	43	44	45	46	47	48	49	50	51	52
	Oct				Nov					Dec			
Mo	28	5	12	19	26			16	23	30		14	21
Tu								Ions setup					
We							TS3						
Th										IONS		Technical stop	
Fr						MD 3							Xmas
Sa													
Su													

Few Short Technical Stops

Stops rare

DC essential, then



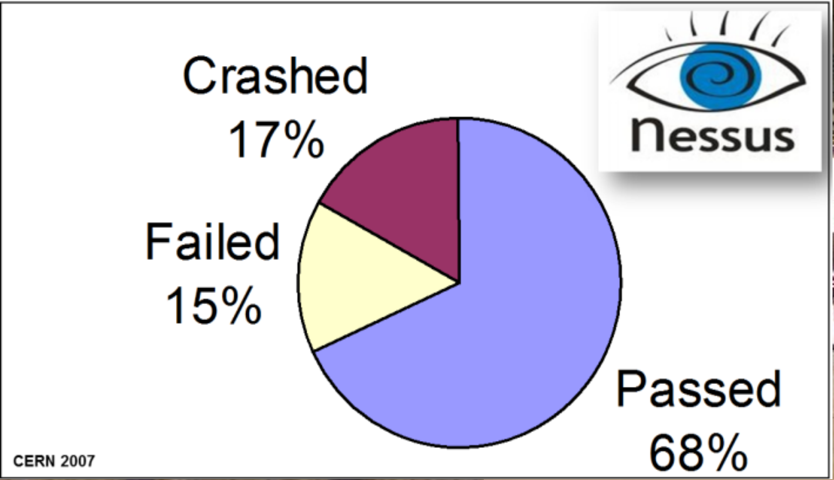
```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xE0F57EA2,0x00000000,0xE0C25C10,0x00000000)


Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

How to prioritize?

- ➔ Delegation of reponsibility
- ➔ Failing prompt patching

Own JavaWebStart

Few Short Technical Stops



Still lack of robustness

→ Small vendors ignore security

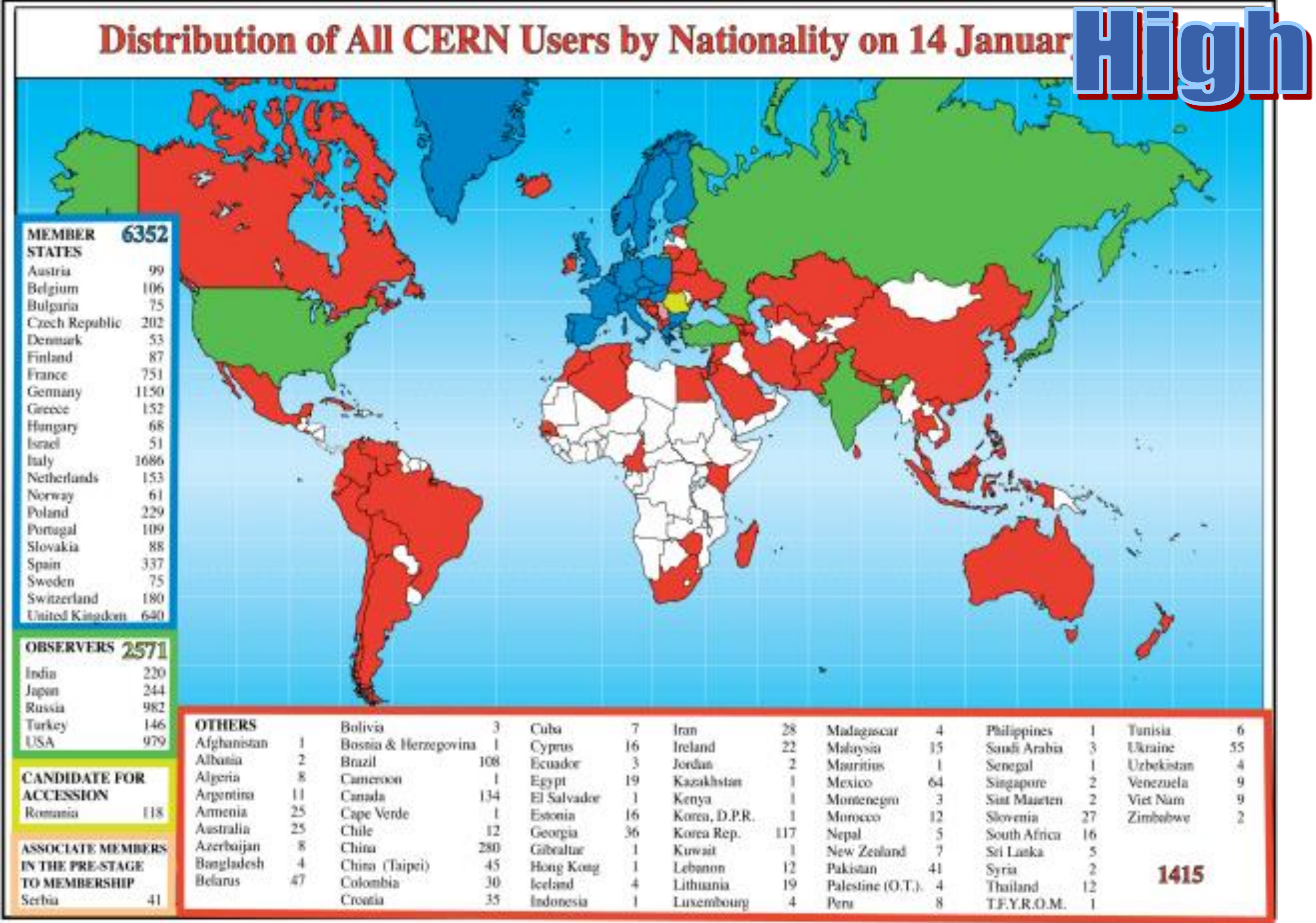
Security demands in tenders

→ Impossible to buy

Pentest everything

→ NMAP vs. LHC: 1:0

High turn-over



Distribution of All CERN Users by Nationality on 14 Januar

MEMBER STATES	6352
Austria	99
Belgium	106
Bulgaria	75
Czech Republic	202
Denmark	53
Finland	87
France	751
Germany	1150
Greece	152
Hungary	68
Israel	51
Italy	1686
Netherlands	153
Norway	61
Poland	229
Portugal	109
Slovakia	88
Spain	337
Sweden	75
Switzerland	180
United Kingdom	640

OBSERVERS	2571
India	220
Japan	244
Russia	982
Turkey	146
USA	979

CANDIDATE FOR ACCESSION	
Romania	118

ASSOCIATE MEMBERS IN THE PRE-STAGE TO MEMBERSHIP	
Serbia	41

OTHERS	1415
Afghanistan	1
Albania	2
Algeria	8
Argentina	11
Armenia	25
Australia	25
Azerbaijan	8
Bangladesh	4
Belarus	47
Bolivia	3
Bosnia & Herzegovina	1
Brazil	108
Cameroon	1
Canada	134
Cape Verde	1
Chile	12
China	280
China (Taipei)	45
Colombia	30
Croatia	35
Cuba	7
Cyprus	16
Ecuador	3
Egypt	19
El Salvador	1
Estonia	16
Georgia	36
Gibraltar	1
Hong Kong	1
Iceland	4
Indonesia	1
Iran	28
Ireland	22
Jordan	2
Kazakhstan	1
Kenya	1
Korea, D.P.R.	1
Korea Rep.	117
Kuwait	1
Lebanon	12
Lithuania	19
Luxembourg	4
Madagascar	4
Malaysia	15
Mauritius	1
Mexico	64
Montenegro	3
Morocco	12
Nepal	5
New Zealand	7
Pakistan	41
Palestine (O.T.).	4
Peru	8
Philippines	1
Saudi Arabia	3
Senegal	1
Singapore	2
Sint Maarten	2
Slovenia	27
South Africa	16
Sri Lanka	5
Syria	2
Thailand	12
T.F.Y.R.O.M.	1
Tunisia	6
Ukraine	55
Uzbekistan	4
Venezuela	9
Viet Nam	9
Zimbabwe	2

High turn-over

Controls experts: No security

IT freshmen: No security

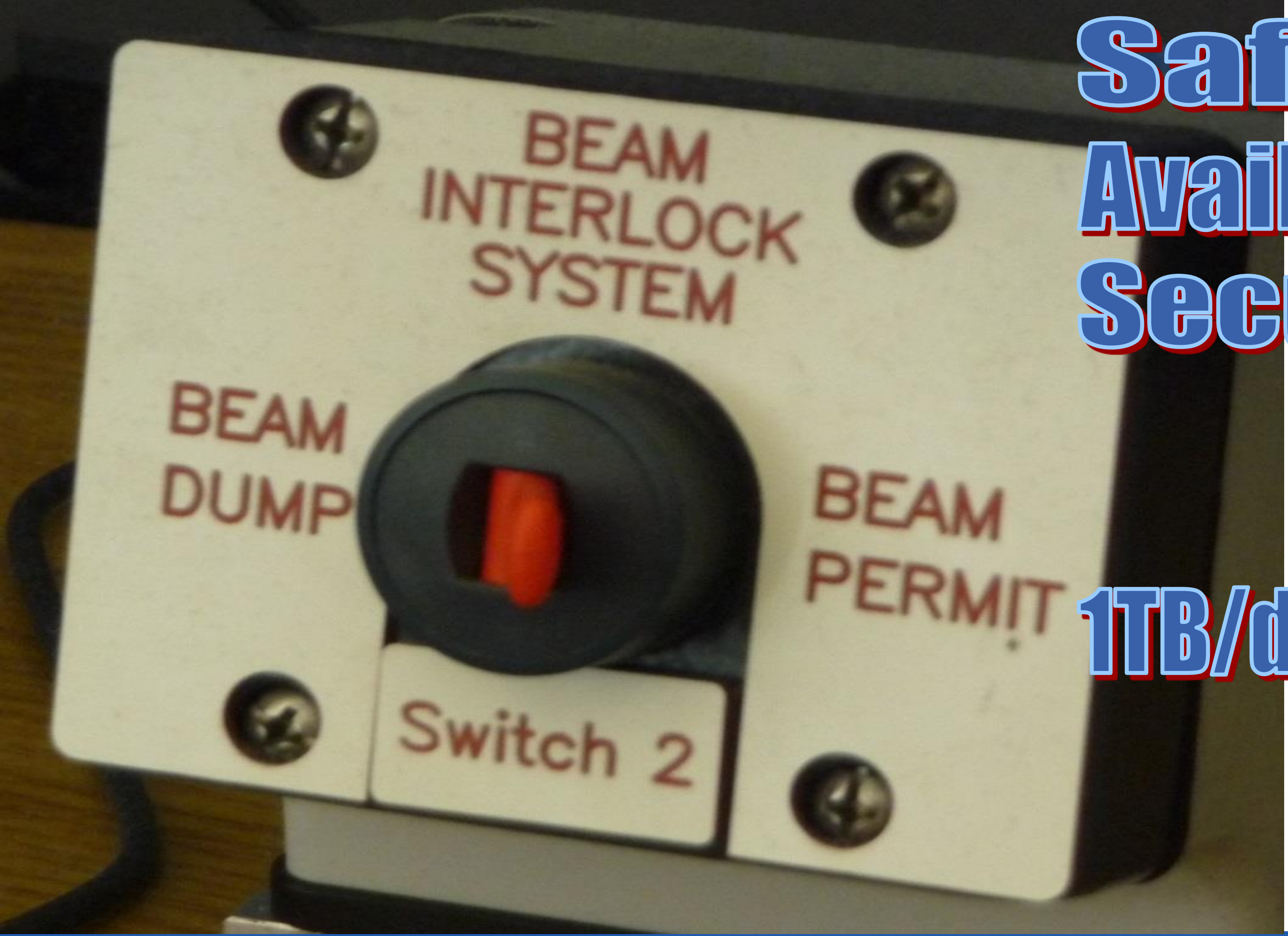
Few SDLCs, if…

Training!

KIPS

CERN WhiteHats

Suboptimal Education

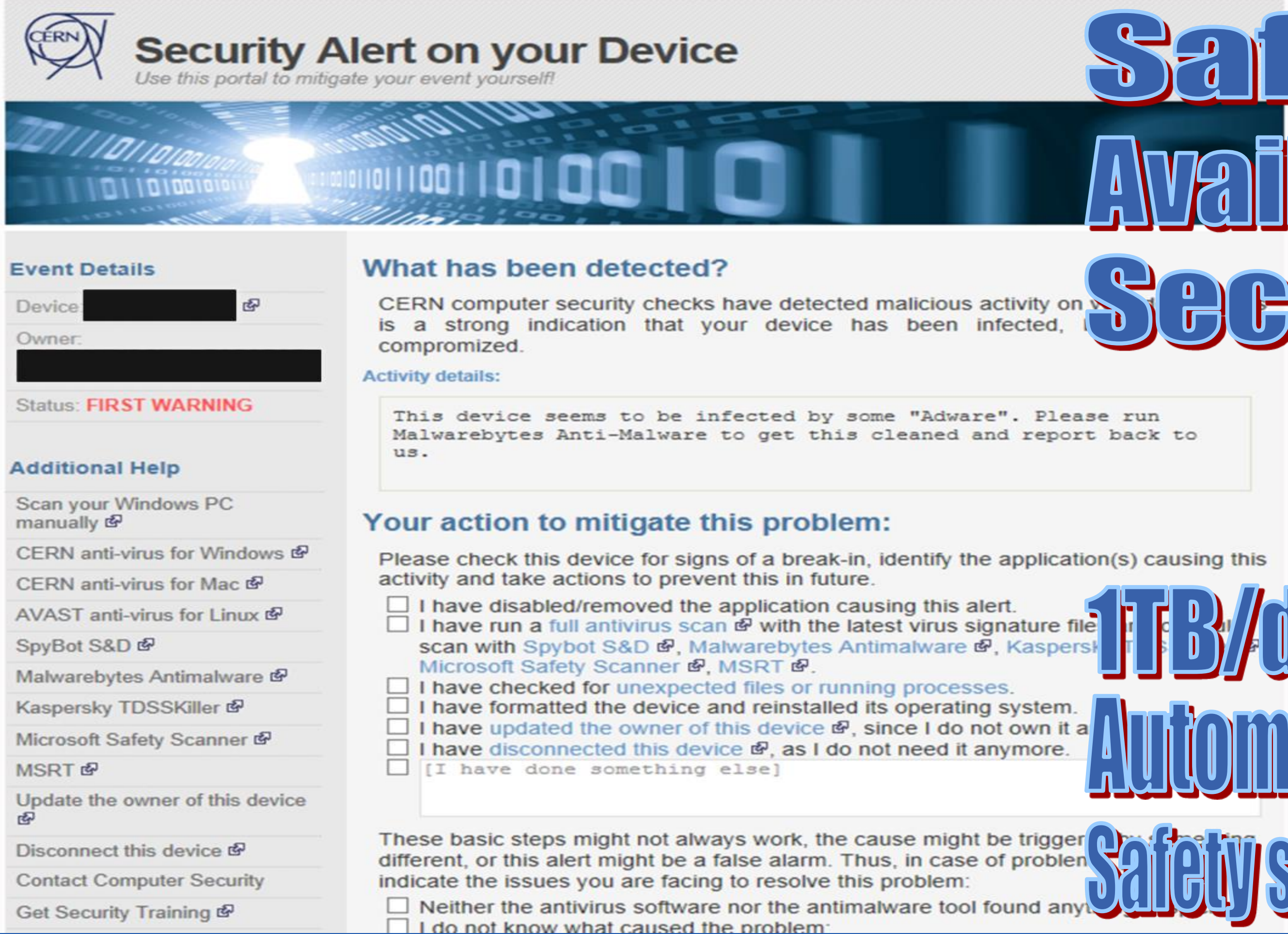


Safety first
Availability next
Security third

1TB/d security data

The Proper Balance

The Proper Balance



Security Alert on your Device

Use this portal to mitigate your event yourself!

Event Details

Device: [redacted]

Owner: [redacted]

Status: FIRST WARNING

Additional Help

- Scan your Windows PC manually
- CERN anti-virus for Windows
- CERN anti-virus for Mac
- AVAST anti-virus for Linux
- SpyBot S&D
- Malwarebytes Antimalware
- Kaspersky TDSSKiller
- Microsoft Safety Scanner
- MSRT
- Update the owner of this device
- Disconnect this device
- Contact Computer Security
- Get Security Training

What has been detected?

CERN computer security checks have detected malicious activity on y is a strong indication that your device has been infected, compromized.

Activity details:

```
This device seems to be infected by some "Adware". Please run
Malwarebytes Anti-Malware to get this cleaned and report back to
us.
```

Your action to mitigate this problem:

Please check this device for signs of a break-in, identify the application(s) causing this activity and take actions to prevent this in future.

- □ I have disabled/removed the application causing this alert.
- □ I have run a full antivirus scan with the latest virus signature file scan with Spybot S&D, Malwarebytes Antimalware, Kaspersk Microsoft Safety Scanner, MSRT.
- □ I have checked for unexpected files or running processes.
- □ I have formatted the device and reinstalled its operating system.
- □ I have updated the owner of this device, since I do not own it a
- □ I have disconnected this device, as I do not need it anymore.
- □ [I have done something else]

These basic steps might not always work, the cause might be trigger different, or this alert might be a false alarm. Thus, in case of problen indicate the issues you are facing to resolve this problem:

- □ Neither the antivirus software nor the antimalware tool found any
- □ I do not know what caused the problem:

Safety first

Availability next

Security third

1TB/d security data

Automatic notifications

Safety systems impede APTs

LHC one-time prototype:
agile/permanent develop’t

High complexity.
But this also
adds protection

World-wide endeavor:
remote expertise
needs access

Availability counts:
Delegation of responsibility

This is a “people” problem!
Training *is* essential…

CERN

www.cern.ch