European Organization for Particle Physics

Exploring the frontiers of knowledge

Finding the Balance between Academic Freedom, Operations & Security

Dr. Stefan Lüders
CERN Computer Security Officer

Journée informatique d'IN2P3, 2020/11/19

Scope:

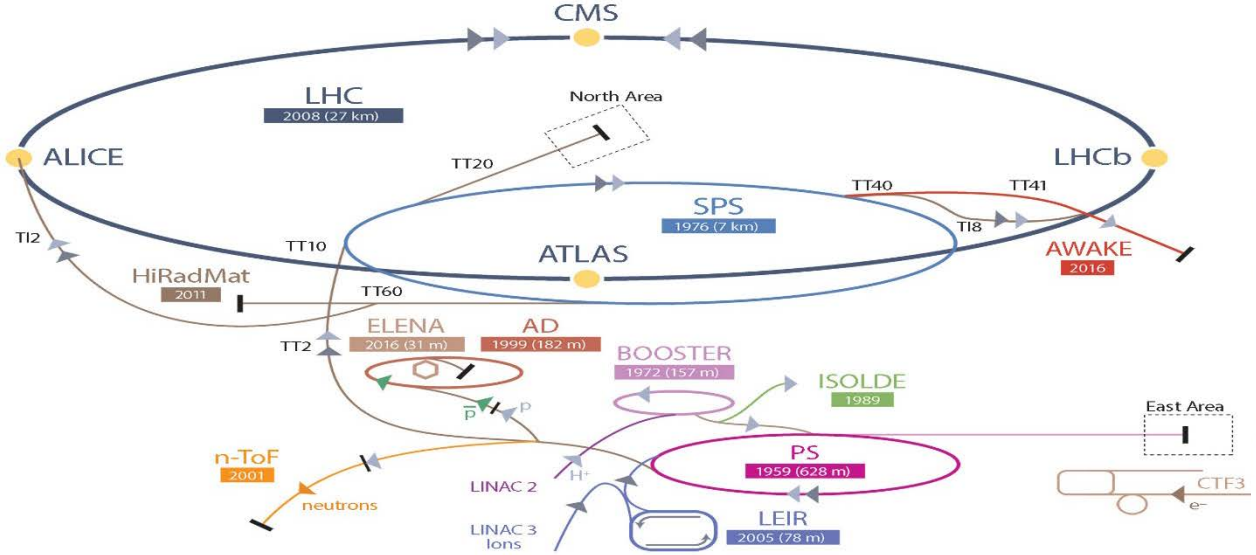
CERN – Know your (security) footprint

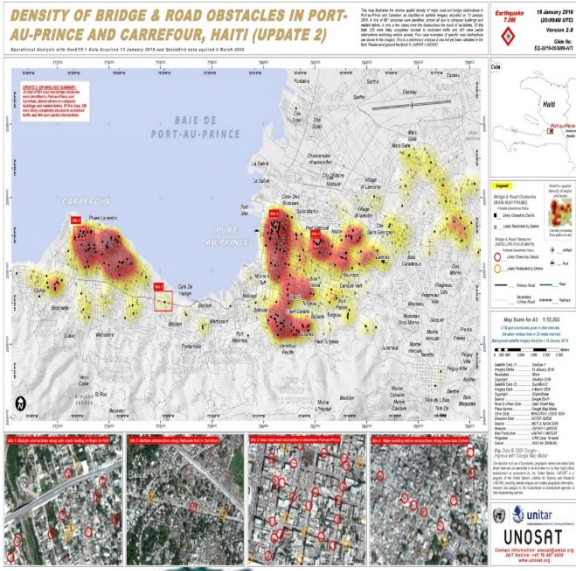
Risks:

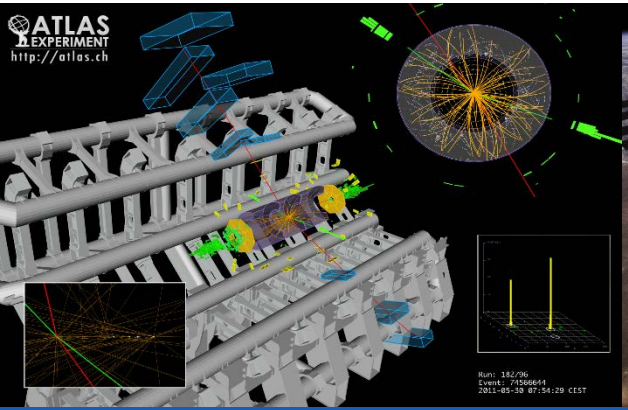
Adversaries & Limitations

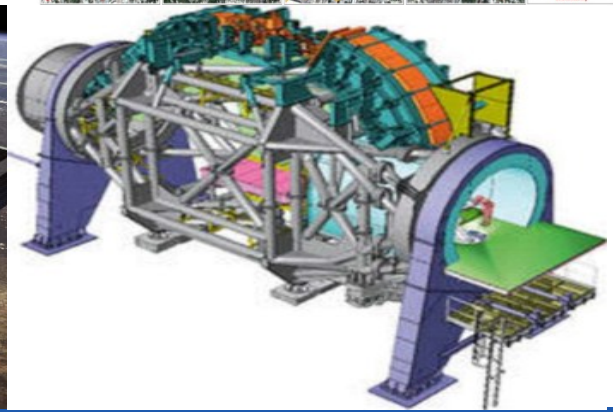
Controls:

Prevention/Protection, Detection & Response

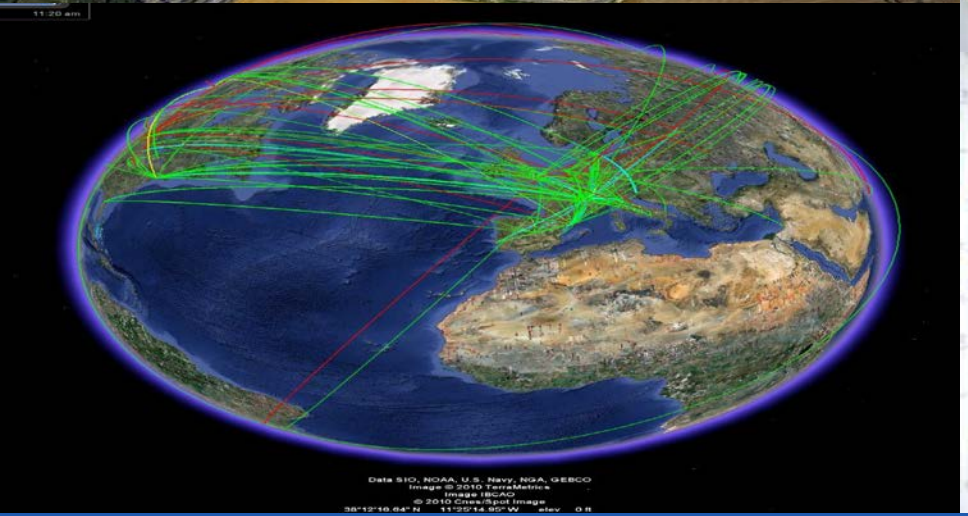

CMS
LHC
2008 (27 km)
North Area
ALICE
LHCb
TT20
TT40
TT41
SPS
1976 (7 km)
TI2
TT10
TI8
ATLAS
AWAKE
2016
HiRadMat
2011
TT60
ELENA
2016 (31 m)
AD
1999 (182 m)
TT2
BOOSTER
1972 (157 m)
ISOLDE
1989
East Area
p
p
n-ToF
2001
PS
1959 (628 m)
CTF3
e⁻
H⁺
neutrons
LINAC 2
LINAC 3
Ions
LEIR
2005 (78 m)


DENSITY OF BRIDGE & ROAD OBSTACLES IN PORT-AU-PRINCE AND CARREFOUR, HAITI (UPDATE 2)
BAIE DE PORT-AU-PRINCE
CARREFOUR
PORT-AU-PRINCE
unitar
UNOSAT

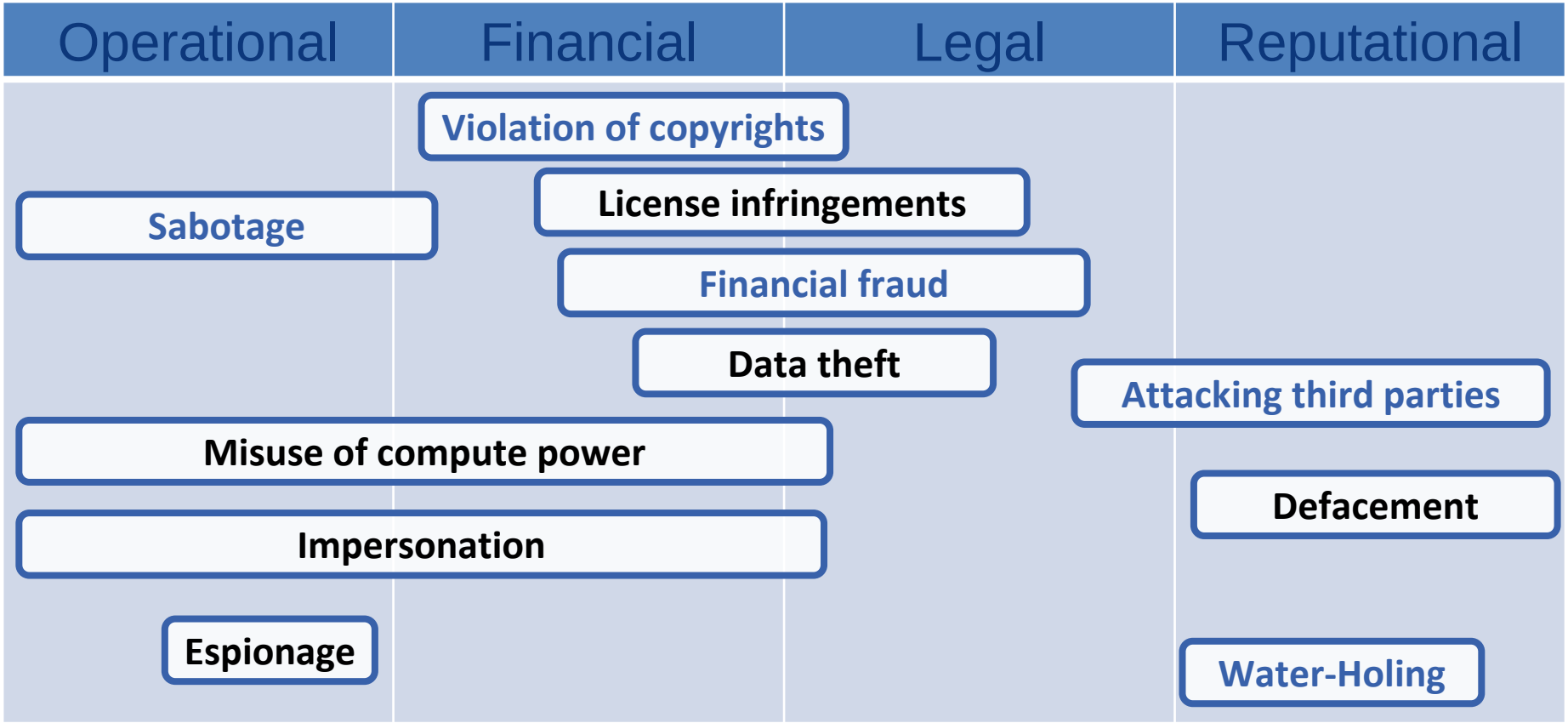

ATLAS EXPERIMENT
http://atlas.ch



A Worldwide Endeavour

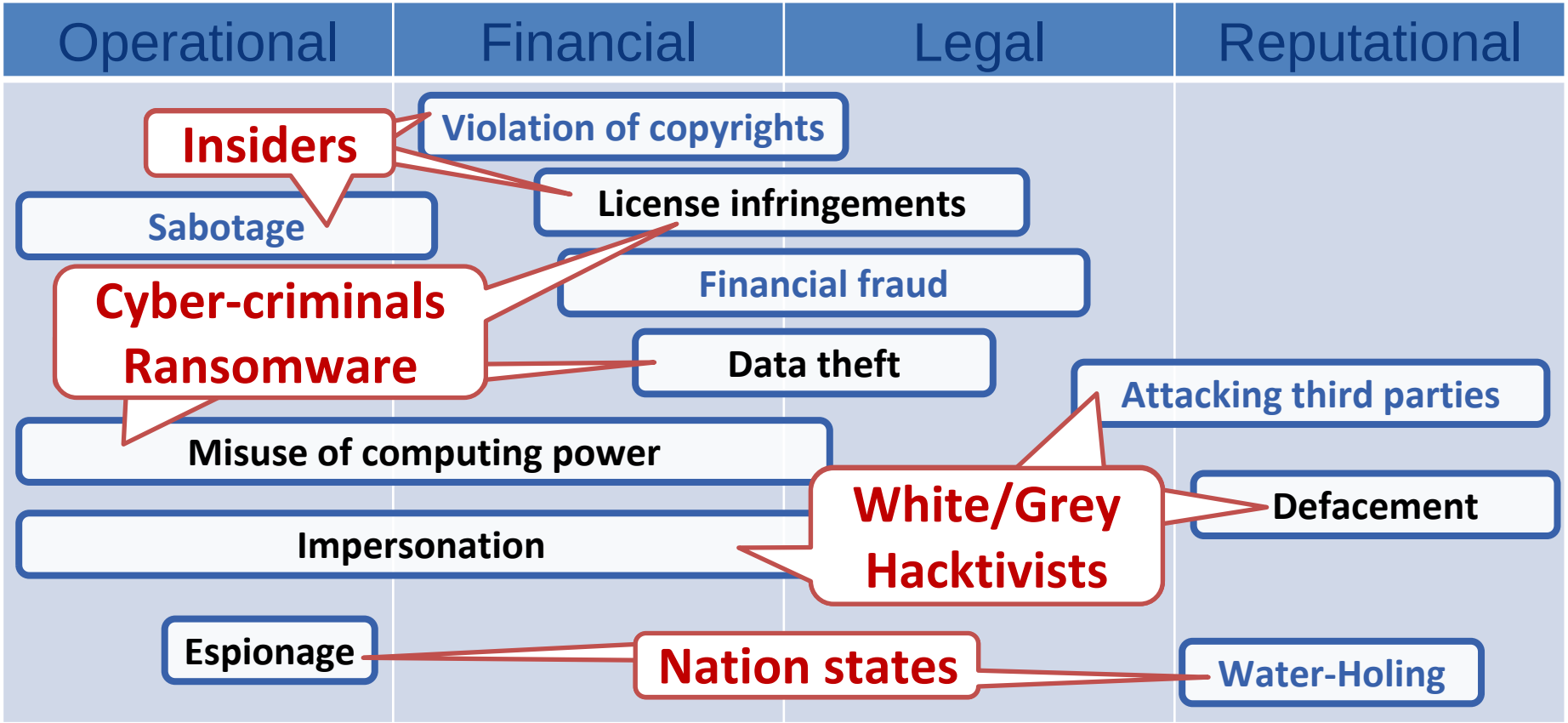


Sectors of “Security” Operation



The “Security” Risk Matrix

Like any other company, organization or university, CERN is under permanent attack.



Adversaries & Motivation

Scope:

CERN – Know your (security) footprint

Risks:

Adversaries & Limitations

Controls:

Prevention/Protection

Mandate:

Protect the operations and reputation of CERN against cyber-threats

Find an appropriate balance between
academic freedom, operations & security.

“Academic Freedom” implies “Responsibility”!

CERN Cyber-Security is everyone’s responsibility
and not that of the Computer Security Officer alone!

Responsibility can be (partially) delegated to CERN’s IT department.

The Computer Security Team acts as facilitator & enabler.

We help people to do their job securely. We secure CERN.
We take over responsibility when handling security incidents.

Governance: Basic Paradigms

Transparency is paramount for successfully running an ethical and trustworthy Computer Security Team.

https://cern.ch/security/home/en/privacy_statement.shtml

Digital Privacy Statement of CERN's Computer Security Team

2016/11/15 by CSO

Introduction

The CERN Computer Security Team ("the Team") takes great care to protect the personal data collected or accessed by us. This Privacy Statement describes how and when the Team gathers, accesses, uses and shares information about you or your usage of CERN's computing facilities and how the Team protects this information.

Scope

This Privacy Statement applies to all persons accessing or using CERN computing facilities, including websites hosted at CERN. It complements the CERN's Computing Rules, i.e. the Operational Circular No. 5 on the Use of CERN Computing Facilities, in particular its subsidiary rules, and Administrative Circular No. 10 on Personal Data Protection.

Information Collection and Use

The CERN Computer Security Team automatically records information ("Log Data") created by your use of CERN's computing facilities in order to detect and understand any abuse of CERN's computing facilities as well as any other violation of the CERN Computing Rules in real time and/or in retrospect.

Log Data contains information on your digital access to CERN's computing facilities including access to the wired and wireless networks, unencrypted network traffic of your device(s) with external services on the Internet, as well as all your activities linked to CERN's interactive computing clusters and its web services. Log Data is always registered with an accurate time stamp. In detail, Log Data includes:

- Usage information when connecting your device(s) to CERN's wired or wireless networks (i.e. ARP and DHCP meta data);

Information Security and Retention

Log Data is stored using the computing facilities provided by CERN's IT department. CERN makes best efforts to protect this Log Data from unauthorized access, or alteration, disclosure or destruction (also see CERN's Digital Privacy Statement). Past experience has shown that a retention period of one year is sufficient to perform the analysis of security related events in retrospect, but this is subject to periodical reviews. Log Data linked with any abuse of CERN's computing facilities as well as any other violation of the CERN Computing Rules is kept indefinitely.

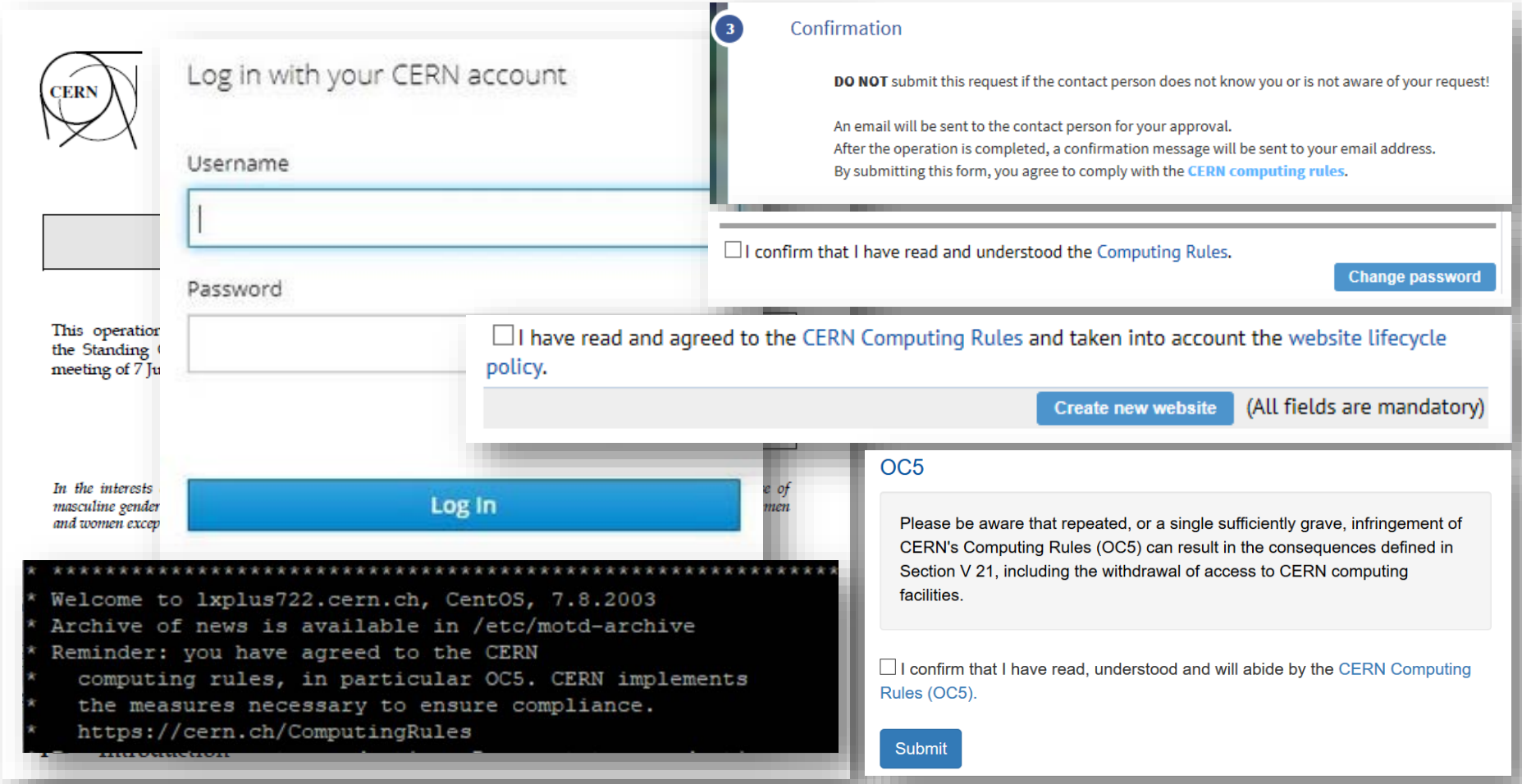
Information Access, Sharing and Disclosure

As stipulated in the CERN Computing Rules, access to Log Data is limited to members of the CERN Computer Security Team, i.e. a limited number of individuals appointed ad-personam by CERN's Computer Security Officer, and only authorized when suspicious activity or activity potentially violating CERN's Computing Rules related with your activity, account(s) or device(s) has been detected by or reported to the Team. In those cases, the Team may preserve or disclose your information only if deemed by CERN to be necessary for legal purposes; to protect the safety of any person; to address fraud, security or technical issues; or to protect CERN's rights or property. In particular, the Team reserves the right to disclose (parts of) your data promptly to third parties in order to avert any further harm to you, your account(s), your device(s) or your data.

Revisions

This Privacy Statement may be periodically revised. Prior versions of the Privacy Statement will be archived and kept available.

https://cern.ch/ComputingRules



Governance: Computing Rules

https://cern.ch/resources

Accounts

Name, mail, login or ID

Search login only

Website review

Please review the sta

Websit

Sh

Websi

apeg

aprilfo

Devic

- Devi
- Loca
- Manu
- Mod
- Gene
- Desc
- Tag:
- Seria
- Oper
- CER
- Netw
- Resp
- Main
- HCP
- IPv6
- Last changed:

New Firewall Opening Request

You are requesting an opening in the main CERN Firewall to allow Internet access to your machine. Please be aware that machines directly exposed to the Internet will be continually attacked and create a risk for the rest of the site. To avoid this you should access your machine from off-site using an intermediate gateway system, as described here. In general, you should reach your system via LXPLUS which has additional intrusion checks.

1. Request Information

Interface Name

Interface Name

Service

Dual Web server (HTTP and HTTPS) on ports 80/tcp and 443/tcp

Port number

80, 443

Protoco

TCP

Application

Give the name of the application listening on this port.

HTTP/HTTPS

Expiration Date

This firewall opening, if authorised, will be automatically deleted on this date. The maxi um time span at any given time is two years. You will be notified before expiration in order to reconfirm and prolong this firewall opening.

25-05-2021

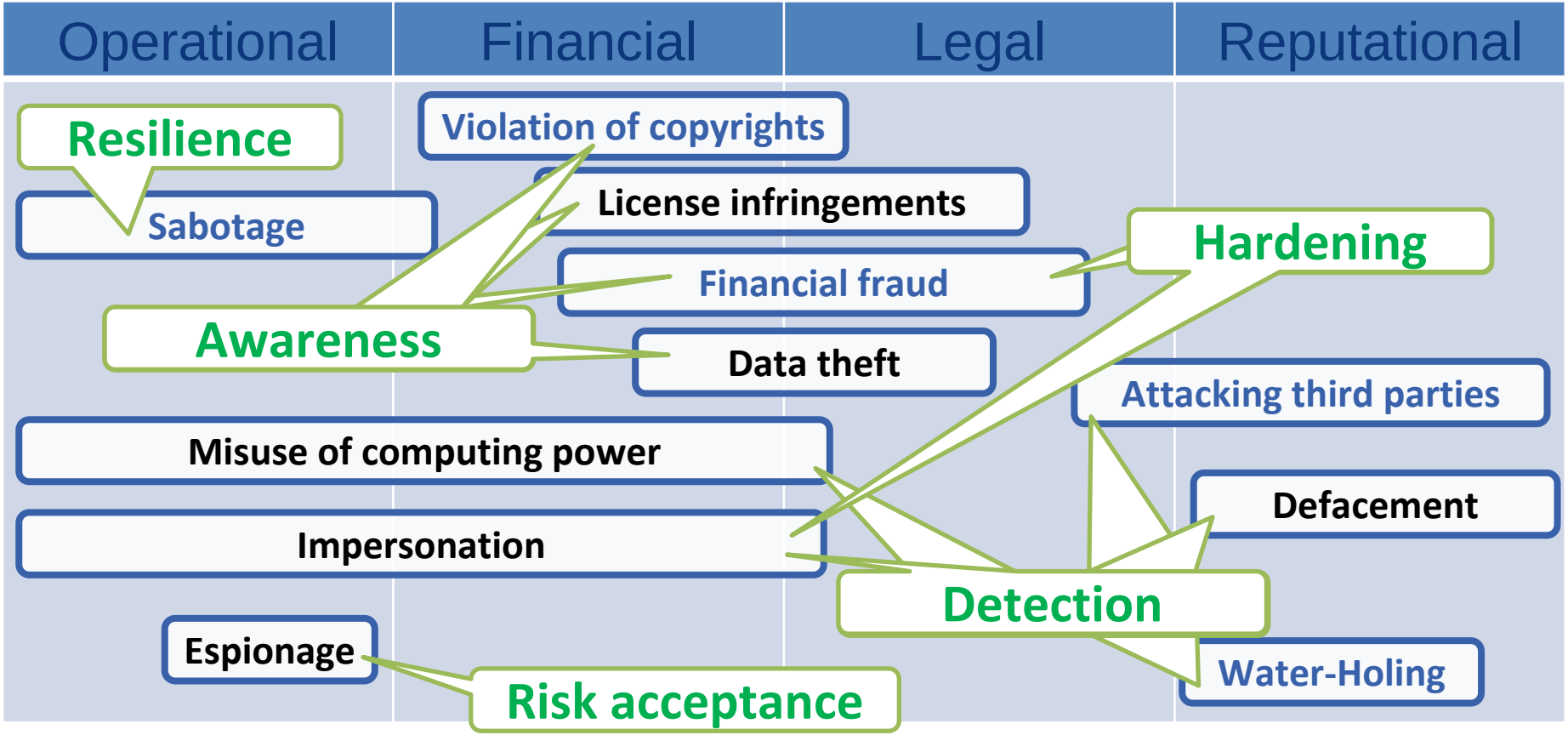
14-07-2016 (10:32)

Firewall: Approval process with pentest & assessment

OpenVAS

skipfish
web application security scanner

Regular verification:
Opened service still listening?
Network traffic to that opening?



Risk Controls

“Home” Awareness

Quelques astuces pour protéger votre ordinateur et vos données

Posters, videos, …you-name-it

Induction & On-Boarding
Mandatory online courses
Technical trainings

Consulting & audits
Pre-Purchase analysis

Protect your computers

Any unprotected computer connected to the Internet is likely to be infected within minutes!

- Keep your system up to date.
- Use anti-virus software.
- Do not install untrusted software.
- your screen with a password.

Let us help you:

Be careful with e-mail & Web

Cybercriminals are trying to trick you!

- Do not open unexpected or suspicious e-mails or attachments.
- Stop-think-click.
- Protect your passwords.
- Do not install untrusted software or plug-ins.

Let us help you:

Protect your passwords

A cybercriminal, who knows your password, will abuse your computing account.

- Never share your passwords with anybody.
- Choose good passwords.
- Do not reuse old passwords.
- Change your passwords regularly.

Let us help you:

Protect your files & data

Cybercriminals are trying to find confidential or sensitive information, also here at CERN.

- Restrict access to your documents and folders.
- Follow the principle of least privilege.
- Do not run file sharing applications.

Let us help you:

Follow the computing rules

Help us to protect CERN's mission and reputation.

- Follow the CERN Computing Rules.
- Take responsibility.
- Do not run restricted applications.
- Respect confidentiality and copyrights.

Let us help you:

Respect copyright

Don't break the law!

- Do not distribute copyrighted material.
- Refrain from file sharing applications or file hosting services.
- Violating copyright is not a trivial offense.
- Protect the Organization.

Let us help you:

https://cern.ch/security/training/en/posters.shtml


EXERCISE ONLY
BREAKING NEWS
CERN - EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH 'VICTIM OF CYBER ATTACK'
Personal details of around 1,000 CERN employees for sale on the dark web
SVN24
FOR EXERCISE PURPOSES ONLY – THIS CLIP CONTAINS FICTITIOUS INFORMATION – FOR E

https://cern.ch/security/recommendations

Static Code Analysis Tools

Below you fin
developers.
quickly, lookir
and non-secu

This is a su
Computer Se
tool
sele
And

The
ava
Gitl
prov
for

C / C

Cp

Fla

Securing Containers & Pods

Often people who are new to container and orchestration technologies are under the impression that these products are inherently secure and suitable for production use. While that might not be true, these solutions offer a lot of configuration options for strengthening the security of the containerized environment in order to get protections similar to that of a virtual machine. This way you can ensure that, even if an attacker

How to keep secrets secret (Alternatives to Hardcoding Passwords)

"Hardcoding passwords" is a short name for putting non-encrypted (plain text) passwords and other secret data (like private keys etc.) into the source code. Typical examples could be:

```
...
private static String passwd = "mYv3rYSECr3tPWD";
...
db = MySQLdb.connect(host="db.server.com", user="admin",
passwd="NOBODYwillEVERguess", db="sales")
...
String url = "jdbc:mysql://" + serverName + "/access?user=webclient&
password=ILoveJuliet";
...
for i in 01 02 03 04; do ./remove_temp_files.sh --machine=appserv$i
--rootpassword="*d3H%sS-W"; done
...
```

Although software developers might not realize, in fact their source code is (or

Web Services

Manage your CERN websites

Home | My websites | Service Status

Current site is http://cern.ch/apeg

- Your access level is: **Site owner**
- View details of **apeg**
- Manage this site
- Open website

Toolbox for current site

- Delete **apeg**
- Site Access & Permissions
- View quota usage
- View site statistics
- Download site logs
- Security scan
- Piwik web statistics
- Archive site

https://cern.ch/web

Safety first
Availability next
Security third

Impact & criticality analyses

Rigorous safety systems prevent (malicious) damage, but reduce availabilities

https://cern.ch/security/services/en/whitehats.shtml

University of Applied Sciences and Arts Northwestern Switzerland
School of Engineering

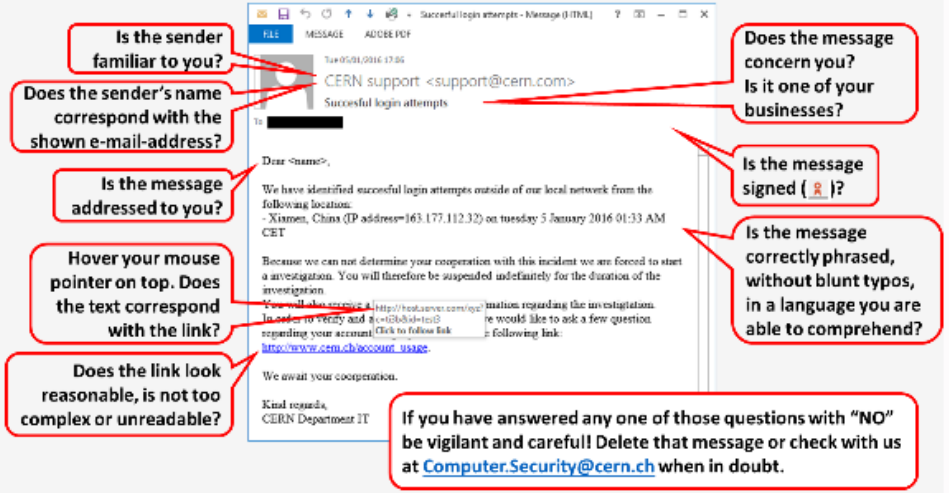
https://cern.ch/security/malicious_email.shtml

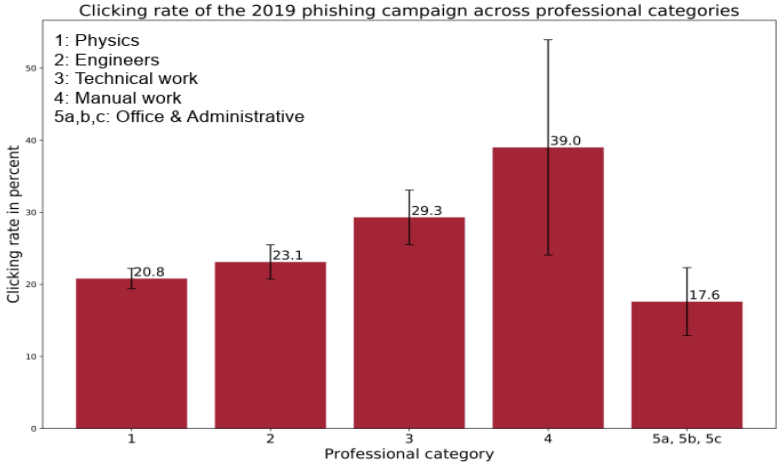
Oops... The link you've just clicked is evil!

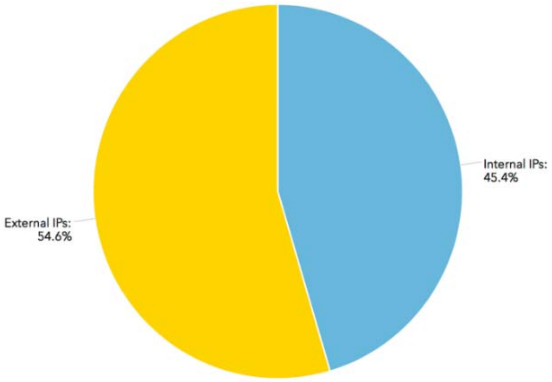
(Version française ici/en-dessous)

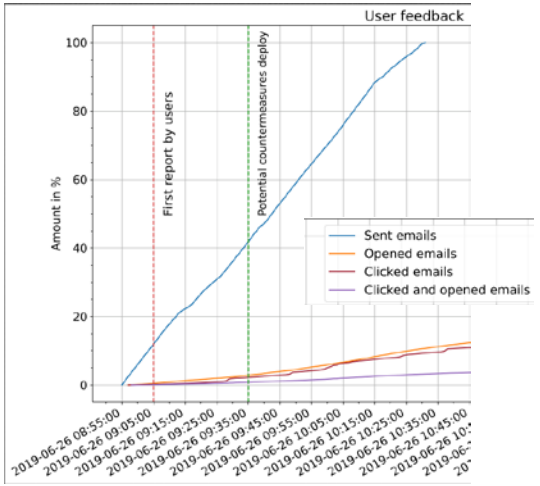
You just fell for a scam. The e-mail whose link you just have clicked is fake. Your "click" could have had severe operational and financial consequences for CERN... Let us explain to you how you can better identify such emails and which consequences clicking on such a malicious link might have for you and your digital assets...

How to identify malicious e-mails









Click rate (2016-2020): ~20.0%

DNS blocking catches only 50%...

...and you have to be quick!

To: cert-snow@cern.ch, service-desk@cern.ch
Subject: [security concern] FW: Testing of new boo

Dear CERN's security experts,

Yesterday I received an email on my cern's account
1) The sender's email address ends with cern.com
2) The
3) The

I was
Please look into it and let me know if there is something to worry about.

To: cert-snow@cern.ch
Subject: FW: Succesful login attempts

This seems a very well done phishing email, using the name of "CERN Depart
Regards,

Subject: FW: Testing of new booking system

Hello,

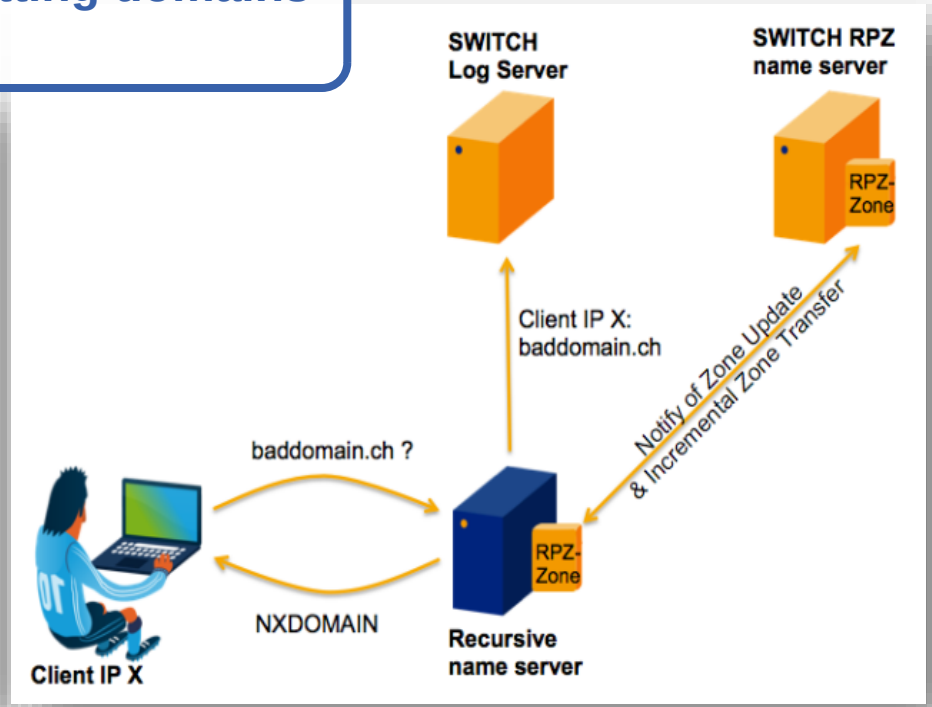
Best Regards

I didn't click, but I forwarded it to a colleague and he clicked it to see the page...

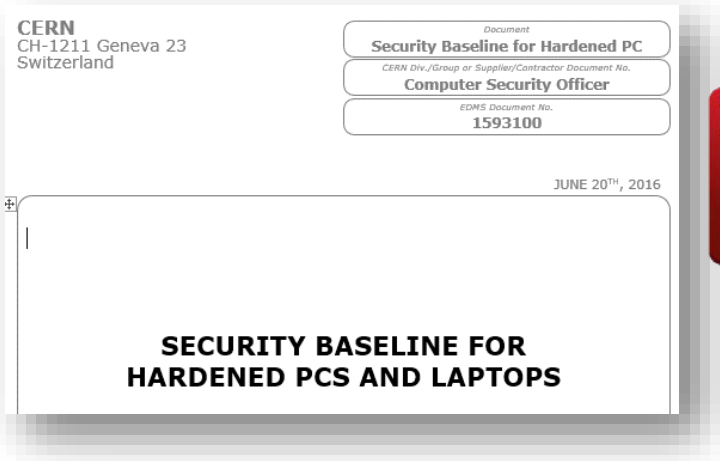
"Clicking Campaign"

Blocking certain malicious & typo-squatting domains in the Domain Name Servers (DNS)

https://cern.ch/security/blocked.shtml



Synchronizing with SWITCH's list of bad domains


CERN
CH-1211 Geneva 23
Switzerland

Document
Security Baseline for Hardened PC

CERN Div./Group or Supplier/Contractor Document No.
Computer Security Officer

EDMS Document No.
1593100

JUNE 20TH, 2016

SECURITY BASELINE FOR
HARDENED PCS AND LAPTOPS

PC Hardening & Alternative PDF Reader

Dedicated appliance to block sophisticated malicious emails & attachments

Scope:

CERN – Know your (security) footprint

Risks:

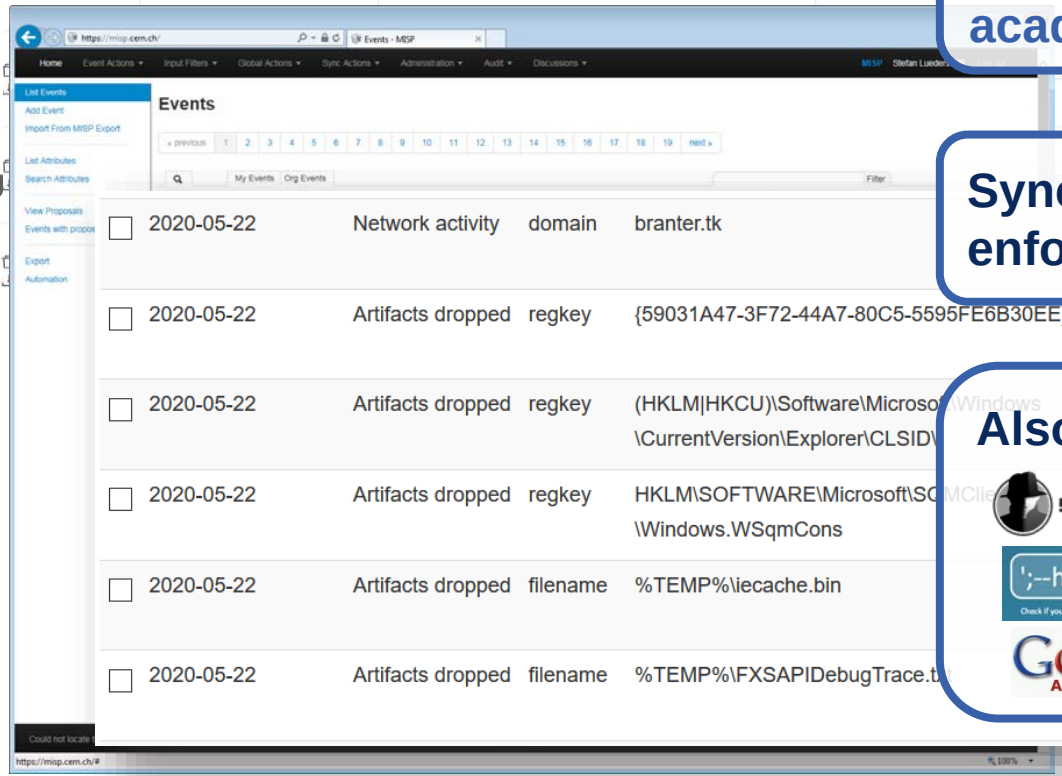
Adversaries & Limitations

Controls:

Prevention/Protection, Detection

FireEye
Email Security

MISP
Threat Sharing

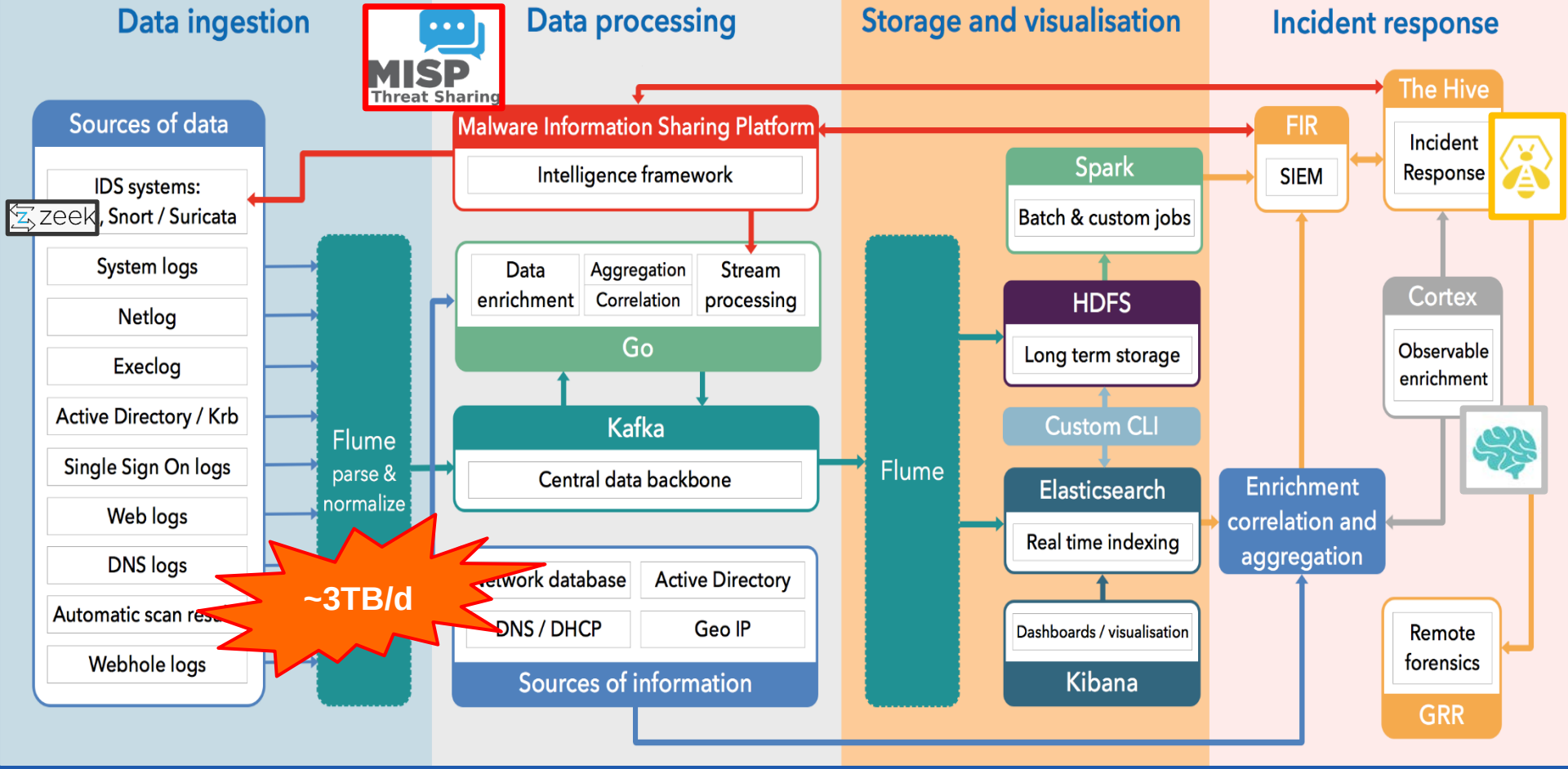


Serving CERN, the WLCG and the HEP and academic community

Synchronized with CH law enforcement & CH CERTs

Also from external feeds:

shadowserver SWITCH ';--have i been pwned? xssed zone-h Google Alerts spamcop.net



The SOC Infrastructure

Scope:

CERN – Know your (security) footprint

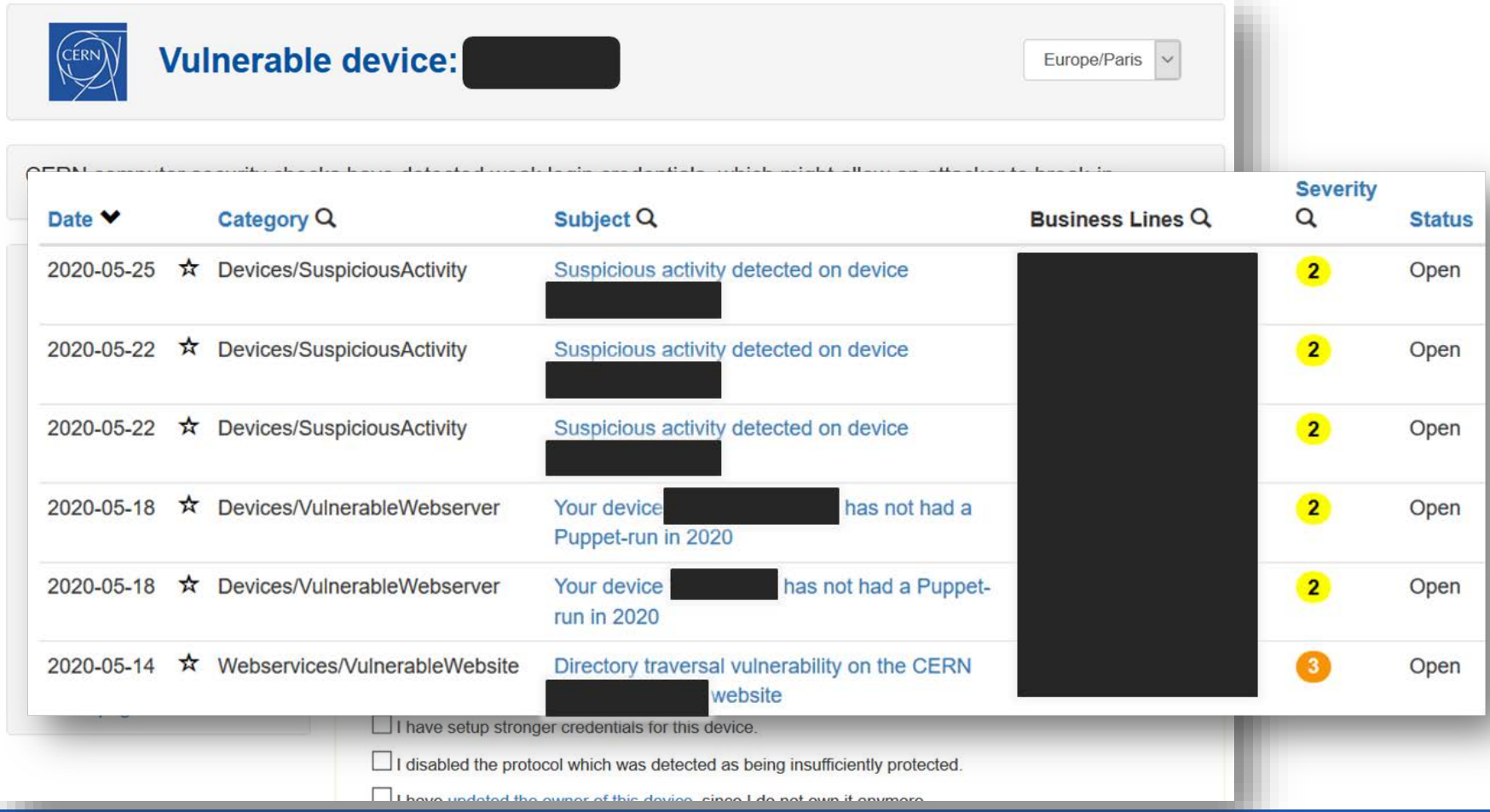
Risks:

Adversaries & Limitations

Controls:

Prevention/Protection, Detection & Response

https://cern.ch/security/services/en/sems.shtml



Vulnerable device: [redacted]

Europe/Paris

Date	Category	Subject	Business Lines	Severity	Status
2020-05-25 ☆	Devices/SuspiciousActivity	Suspicious activity detected on device [redacted]	[redacted]	2	Open
2020-05-22 ☆	Devices/SuspiciousActivity	Suspicious activity detected on device [redacted]		2	Open
2020-05-22 ☆	Devices/SuspiciousActivity	Suspicious activity detected on device [redacted]		2	Open
2020-05-18 ☆	Devices/VulnerableWebserver	Your device [redacted] has not had a Puppet-run in 2020		2	Open
2020-05-18 ☆	Devices/VulnerableWebserver	Your device [redacted] has not had a Puppet-run in 2020		2	Open
2020-05-14 ☆	Webservices/VulnerableWebsite	Directory traversal vulnerability on the CERN [redacted] website		3	Open

☐ I have setup stronger credentials for this device.

☐ I disabled the protocol which was detected as being insufficiently protected.

☐ I have updated the owner of this device, since I do not own it anymore.

"Auto-Notify"

https://cern.ch/security/services/en/emergency.shtml

- Triage
- Taking over service
- Coordinating comm's
- "Avalanching"
- Forensics
- Close out

CERN also provides incident response & forensics services to the WLCG, EGI as well as the HEP and academic community world-wide

CERT & Forensics

https://cern.ch/security/reports/en/monthly_reports.shtml

Computer Security Report for April 2020

Corona Warning Please be extremely skeptical when receiving emails around the subject "Corona"/"COVID-19", in particular if those emails containing links or attachments. STOP --- THINK --- DON'T CLICK! ...and don't open any attachment. If you are in doubt, cross-check with us at Computer.Security@cern.ch.

Blackmailed with your password? If you received recently an email with a password similar to one of yours, claiming that they "know every think about you", and asking you to transfer Bitcoins to them, don't worry and don't answer. This is a scam. The password, eventually a real one, has been exposed in a data breach, likely already a while ago, and was made public in so-called "password dumps" containing of millions of other passwords. The scammers here just took advantage of those dumps to blackmail you. If you recall that password and still use it somewhere, time to change it now. In parallel, we continue to inform owners of exposed passwords if we get hold of similar password dumps... More details can be found in those two Bulletin articles.

iOS/iPhone/iPad Exploit A zero-day vulnerability, i.e. a vulnerability which has not patches ready yet, of the native mail client in the iOS operating system has been reported being actively exploited. Unfortunately, there is no fix out yet. Only option for the moment is avoiding having your emails pushed to your iPhone/iPad ("Settings" -> "Passwords & Accounts" -> have "Fetch New Data: Off" by disabling "Push" and

Monthly Reports

CERN values its open environment

? “Security” delegated to everyone

Like others, permanently under attack

- Training the minds of people
- Keeping inventories & life-cycles
- Being prepared + trying to detect early

www.cern.ch

Thank you for listening!

Questions?