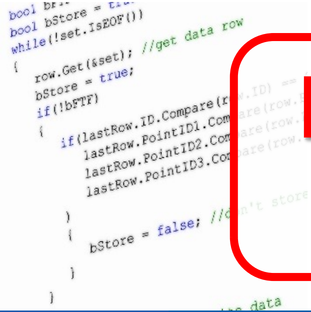
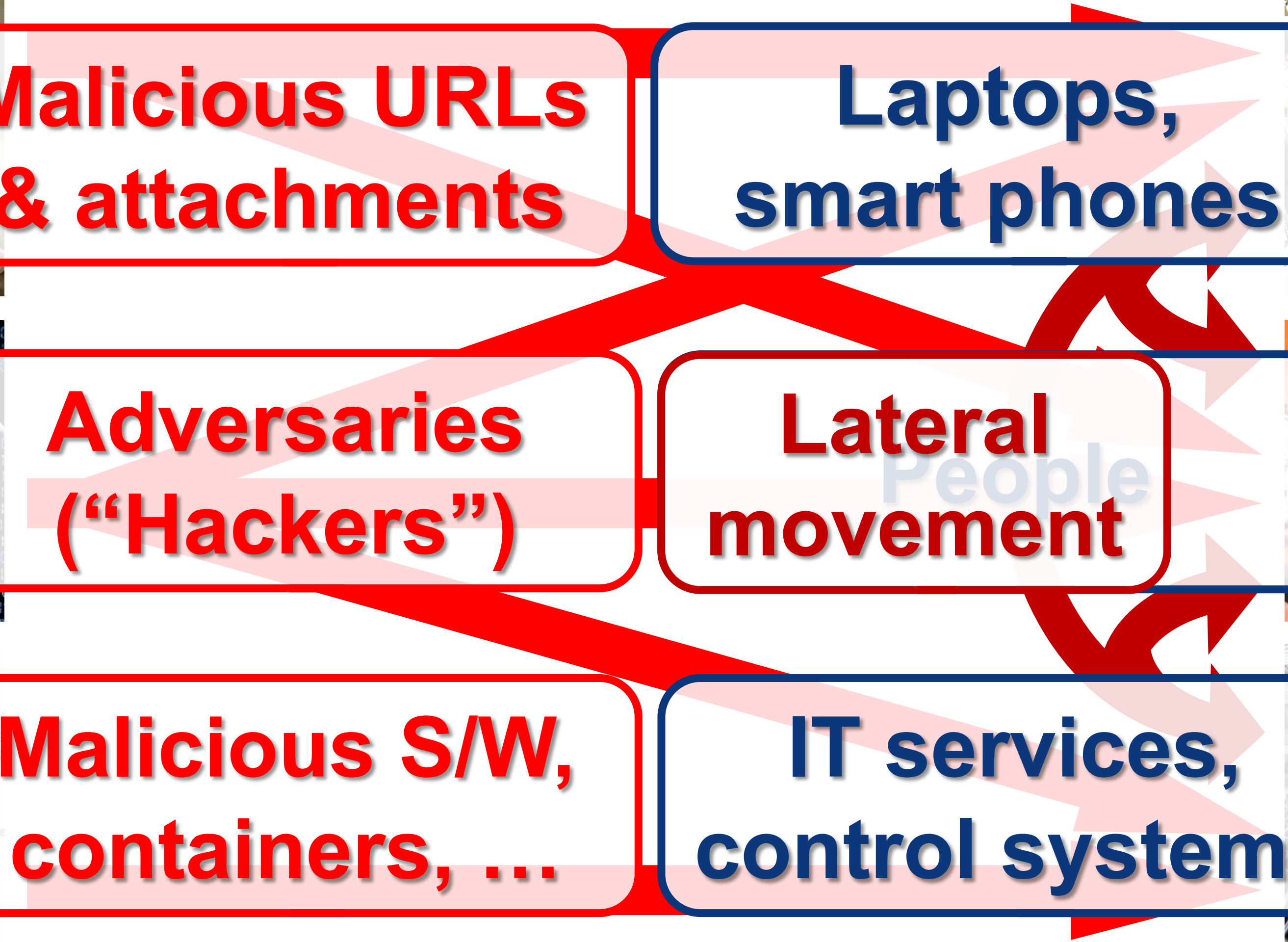
# Computer Security Operations

Computer.Security@cern.ch



```
bool b...  = tru...
bool bStore = ...IsEOF())
while(!set.IsEOF())
{
    row.Get(&set); //get data row
    bStore = true;
    if(!bFTF)
    {
        if(lastRow.ID.Compare(r...
            lastRow.PointID1.Com...
            lastRow.PointID2.Com...
            lastRow.PointID3.Co...
        )
        {
            bStore = false; //don't store
        }
    }
}
```



Malicious URLs & attachments

Adversaries (“Hackers”)

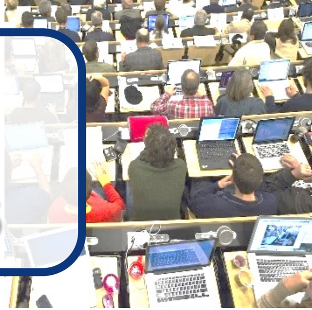
Malicious S/W, containers, …

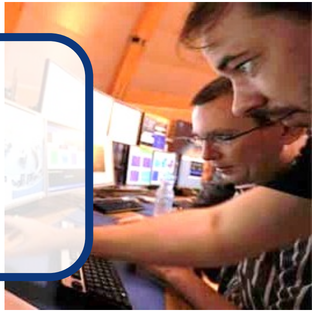
Laptops, smart phones

Lateral movement

People

IT services, control systems

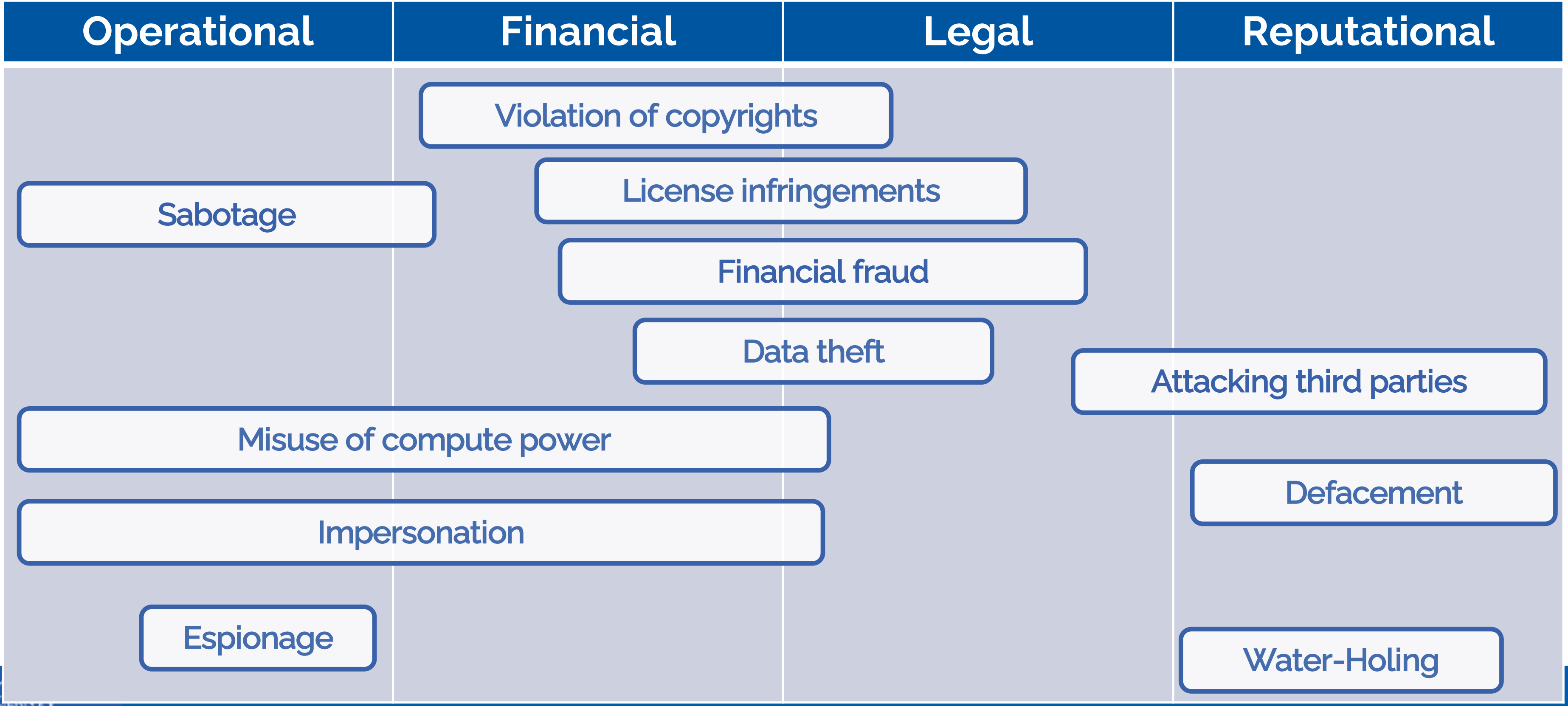




# Primary Attack Vectors

CERN Computer Security Operations
Computer.Security@cern.ch

# RISK MATRIX



Operational

Financial

Legal

Reputational

Violation of copyrights

License infringements

Sabotage

Financial fraud

Data theft

Attacking third parties

Misuse of compute power

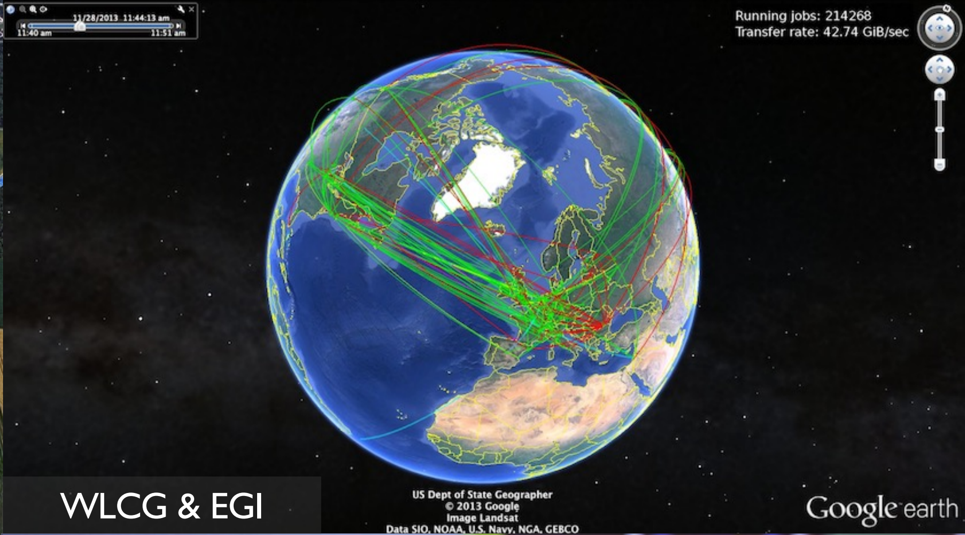
Defacement

Impersonation

Espionage

Water-Holing

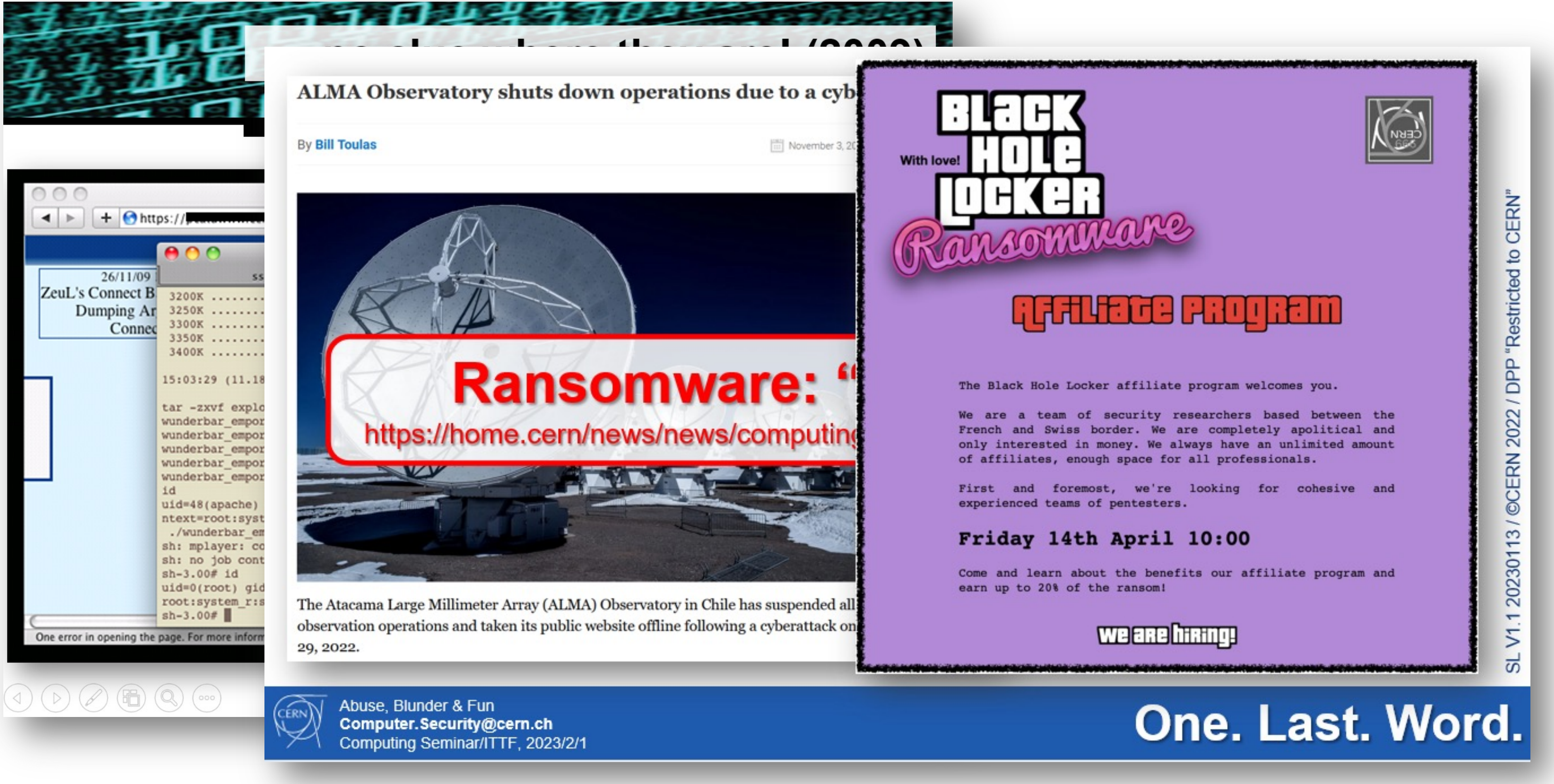
Campus



WLCG & EGI

Data centre

Control systems



26/11/09
ZeuL's Connect B
Dumping Ar
Connec

```
3200K ........
3250K ........
3300K ........
3350K ........
3400K ........

15:03:29 (11.18

tar -zxvf explo
wunderbar_empor
wunderbar_empor
wunderbar_empor
wunderbar_empor
wunderbar_empor
id
uid=48(apache)
ntext=root:syst
 ./wunderbar_em
sh: mplayer: co
sh: no job cont
sh-3.00# id
uid=0(root) gid
root:system_r:s
sh-3.00# █
```

One error in opening the page. For more inform

**ALMA Observatory shuts down operations due to a cyb**

By Bill Toulas November 3, 20

**Ransomware: "**

https://home.cern/news/news/computing

The Atacama Large Millimeter Array (ALMA) Observatory in Chile has suspended all observation operations and taken its public website offline following a cyberattack on 29, 2022.

**BLACK HOLE LOCKER Ransomware**

With love!

**AFFILIATE PROGRAM**

The Black Hole Locker affiliate program welcomes you.

We are a team of security researchers based between the French and Swiss border. We are completely apolitical and only interested in money. We always have an unlimited amount of affiliates, enough space for all professionals.

First and foremost, we're looking for cohesive and experienced teams of pentesters.

**Friday 14th April 10:00**

Come and learn about the benefits our affiliate program and earn up to 20% of the ransom!

**we are hiring!**

Abuse, Blunder & Fun
**Computer.Security@cern.ch**
Computing Seminar/ITTF, 2023/2/1

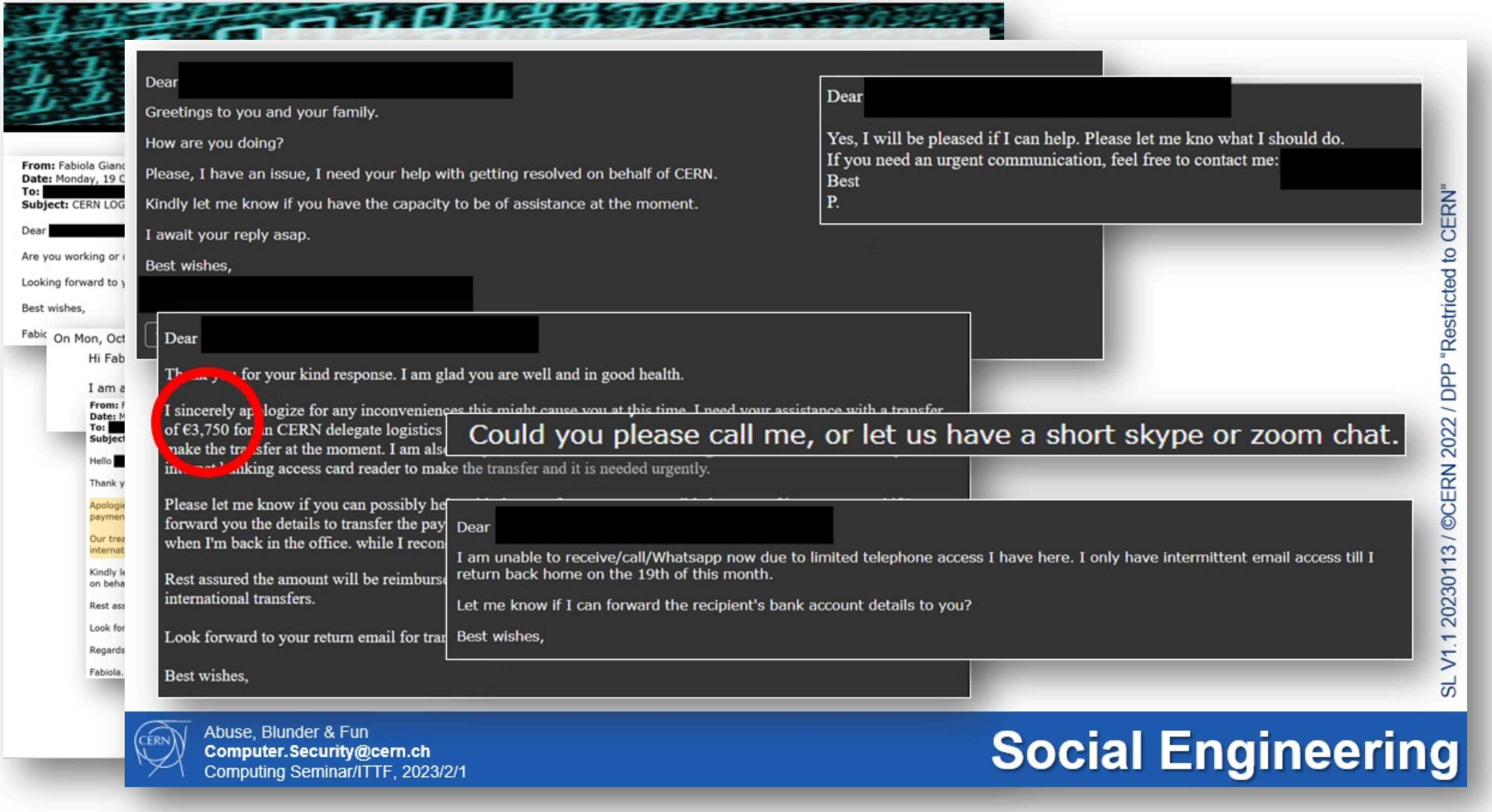
**One. Last. Word.**

SL V1.1 20230113 / ©CERN 2022 / DPP "Restricted to CERN"

CERN Computer Security Operations
**Computer.Security@cern.ch**

# Operational Risks

# Financial Risks



From: Fabiola Gianc
Date: Monday, 19 O
To: [redacted]
Subject: CERN LOG

Dear [redacted]

Are you working or

Looking forward to y

Best wishes,

Fabic

On Mon, Oct
Hi Fab

I am a

From: F
Date: M
To: [redacted]
Subject

Hello [redacted]

Thank y

Apologie
paymen

Our trea
internat

Kindly le
on beha

Rest ass

Look for

Regards

Fabiola.

Dear [redacted]

Greetings to you and your family.

How are you doing?

Please, I have an issue, I need your help with getting resolved on behalf of CERN.

Kindly let me know if you have the capacity to be of assistance at the moment.

I await your reply asap.

Best wishes,

[redacted]

Dear [redacted]

Yes, I will be pleased if I can help. Please let me kno what I should do.
If you need an urgent communication, feel free to contact me: [redacted]
Best
P.

Dear [redacted]

Thank you for your kind response. I am glad you are well and in good health.

I sincerely apologize for any inconveniences this might cause you at this time. I need your assistance with a transfer of €3,750 for an CERN delegate logistics
make the transfer at the moment. I am als
internet banking access card reader to make the transfer and it is needed urgently.

Please let me know if you can possibly he
forward you the details to transfer the pay
when I'm back in the office. while I recon

Rest assured the amount will be reimburs
international transfers.

Look forward to your return email for tra

Best wishes,

Could you please call me, or let us have a short skype or zoom chat.

Dear [redacted]

I am unable to receive/call/Whatsapp now due to limited telephone access I have here. I only have intermittent email access till I return back home on the 19th of this month.

Let me know if I can forward the recipient's bank account details to you?

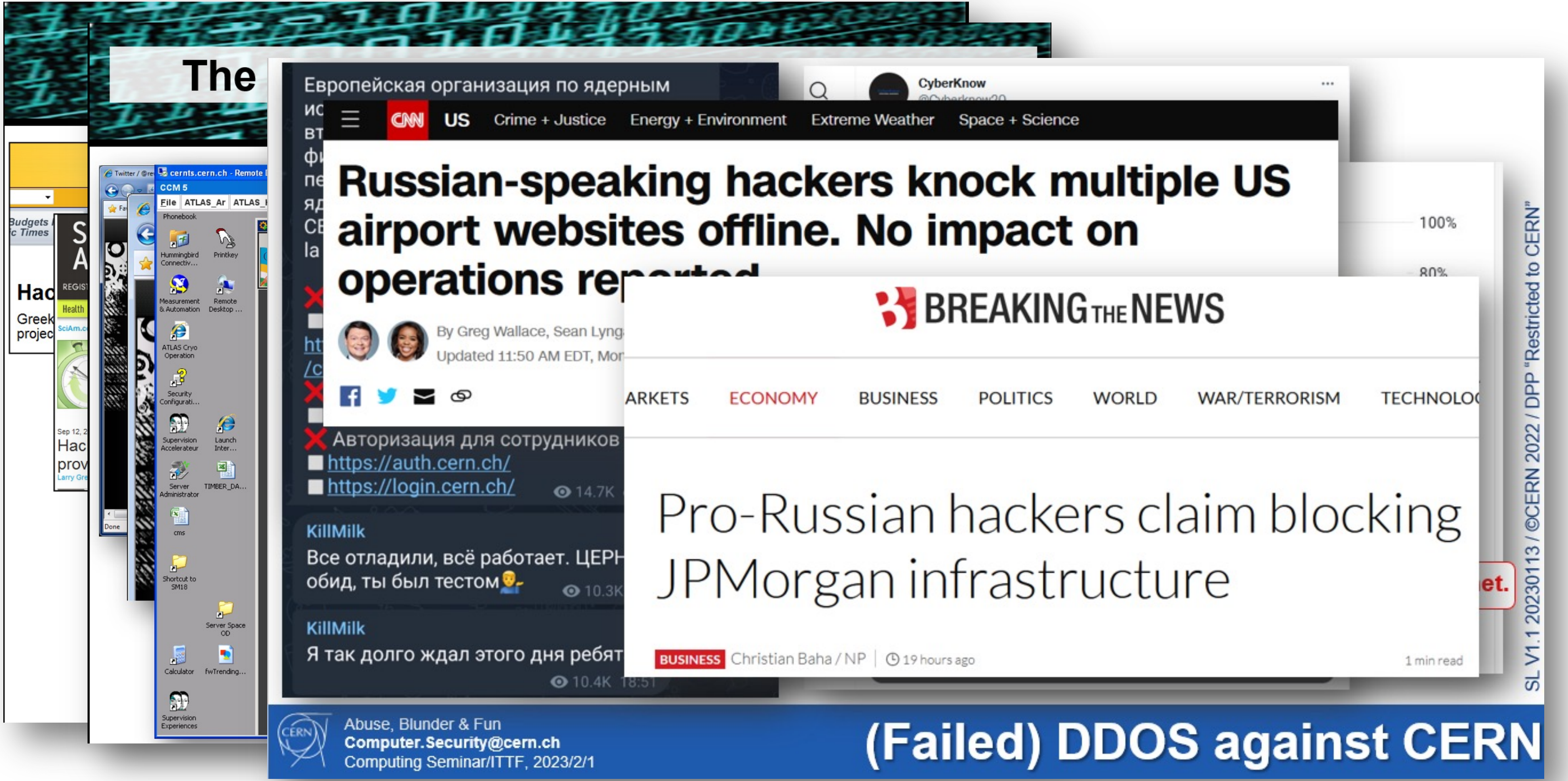
Best wishes,

SL V1.1 20230113 / ©CERN 2022 / DPP "Restricted to CERN"

Abuse, Blunder & Fun
**Computer.Security@cern.ch**
Computing Seminar/ITTF, 2023/2/1

**Social Engineering**

# Reputational Risks



Европейская организация по ядерным
ис
вт
фи
пе
яд
СЕ
la
ht
/c

❌ Авторизация для сотрудников
□ https://auth.cern.ch/
□ https://login.cern.ch/
👁 14.7K

KillMilk
Все отладили, всё работает. ЦЕРН обид, ты был тестом🤷‍♂️
👁 10.3K

KillMilk
Я так долго ждал этого дня ребят
👁 10.4K 18:51

CyberKnow
@Cyberknow20

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

By Greg Wallace, Sean Lyng
Updated 11:50 AM EDT, Mon

Pro-Russian hackers claim blocking JPMorgan infrastructure

BUSINESS Christian Baha / NP | 19 hours ago 1 min read

SL V1.1 20230113 / ©CERN 2022 / DPP "Restricted to CERN"

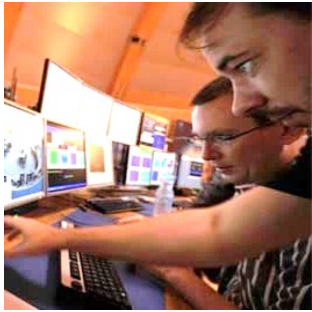
Abuse, Blunder & Fun
**Computer.Security@cern.ch**
Computing Seminar/ITTF, 2023/2/1

**(Failed) DDOS against CERN**

**2008** **2011** **2023**

**Computer Security Team’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. Detect early; respond quickly & thoroughly.

https://home.cern/news/news/computing/computer-security-about-risks-and-threats

# Principles

**Policies:** Maintaining CERN Computing Rules (OC5).

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

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

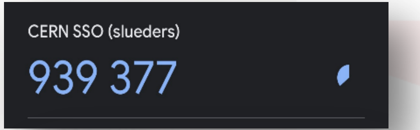
https://home.cern/news/news/computing/computer-security-room-top

**Dedicated Training:** Providing in-depth training on security practices incl. programming (with HR). 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

## Awareness, Training & Policies

# Account Protection



CERN SSO (slueders)

939 377

**2FA:** Deploying extra protection to accounts.

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/d for CERN)

https://home.cern/news/news/computing/computer-security-password-revolutions

## ***EOP — xorlab — MDO* Mail-Filtering:**

Quarantining SPAM & malware

~115k emails analysed per day; 10% SPAM; 2% quarantined; >12/d manually checked (… >50% FP)

https://home.cern/news/news/computing/computer-security-wrong-link-wrong-login-and-boom

## ***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-your-device

***Threatray* Memory Hashing:** Detecting anomalies on CERN-managed devices

~50 devices so far in testing; IT department to come next month

# Endpoint Protection

**Automatic Vulnerability Scanning:**

Identifying weaknesses of endpoints & servers, unused firewall openings, as well as exposed secrets and ransomwared files on file storages.

~24k devices scanned per month; ~210 issues per month; ~12M *EOS* file actions analysed
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*).

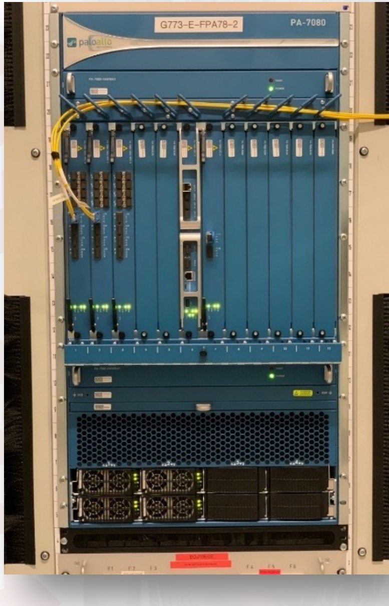
20-30 in-depth reviews per year

**Self-Security Assessment for Cloud Services:**

Providing metrics, guidelines & controls for better security.

Prototype ready. Looking for volunteers to test it

# PenTests, Reviews & Consulting



***PaloAlto* Firewalling:** Performing deep packet inspection and policy-based IP, domain & URL blocking (with IT-CS).

>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 IT-CS & 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.

# Network Protection

## Code / Container Scanning:

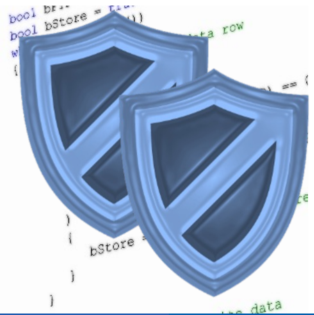
Deploying *GitLab/GitCI* and *Harbor* security features.

“Avoiding salmonella in your code” — Bulletin article to come

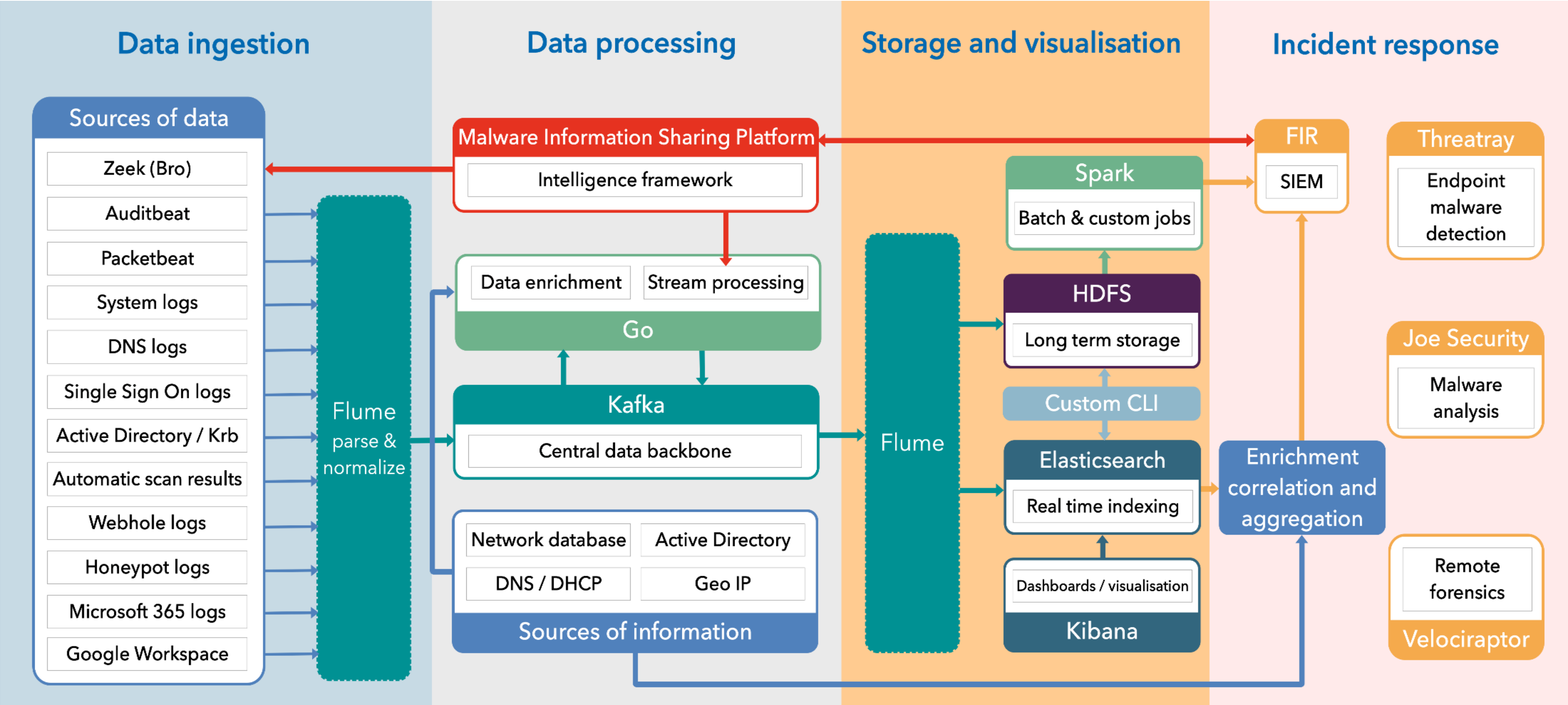
## Software-Bill-of-Materials (SBOM):

Pushing via *CNIC* for a curation service to avoid (automatic) downloading of malicious libraries, packages, containers & VMs. This also improves dependency trees and licensing.

https://home.cern/news/news/computing/computer-security-when-your-restaurant-turns-sour



# Orchestration (the “SOC”)



## Data ingestion

### Sources of data

- Zeek (Bro)
- Auditbeat
- Packetbeat
- System logs
- DNS logs
- Single Sign On logs
- Active Directory / Krb
- Automatic scan results
- Webhole logs
- Honeypot logs
- Microsoft 365 logs
- Google Workspace

Flume parse & normalize

## Data processing

Malware Information Sharing Platform

Intelligence framework

Data enrichment

Stream processing

Go

Kafka

Central data backbone

Network database

Active Directory

DNS / DHCP

Geo IP

Sources of information

## Storage and visualisation

Flume

Spark

Batch & custom jobs

HDFS

Long term storage

Custom CLI

Elasticsearch

Real time indexing

Dashboards / visualisation

Kibana

## Incident response

FIR

SIEM

Enrichment correlation and aggregation

Threatray

Endpoint malware detection

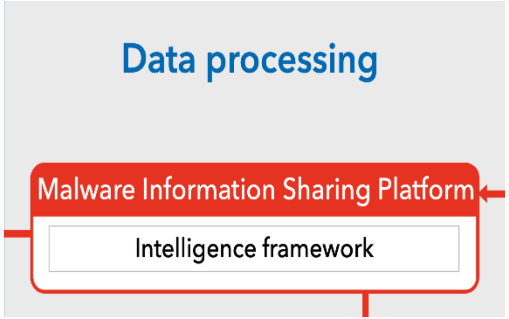
Joe Security

Malware analysis

Remote forensics

Velociraptor

**ThreatIntel:** Obtaining high-quality Indicators of Compromise.

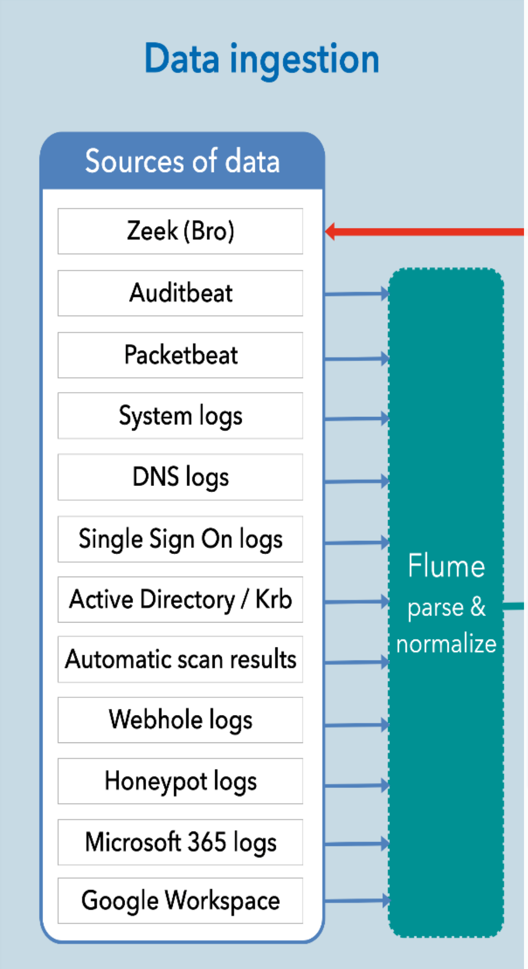


e.g. IPs, domains, file hashes from our peers and security vendors.

~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. this year: 30+ universities world-wide informed of ransomware preparations in their IT infrastructure



Data ingestion

Sources of data

Zeek (Bro)
Auditbeat
Packetbeat
System logs
DNS logs
Single Sign On logs
Active Directory / Krb
Automatic scan results
Webhole logs
Honeypot logs
Microsoft 365 logs
Google Workspace

Flume parse & normalize

# Ingestion, Processing & Storage:

Monitoring traffic at the Internet & TN gates, DNS requests, CERN SSO logins, *LXBATCH/LXPLUS/AIADM* activities, … *Google* Workspace & *MS Azure* to come.

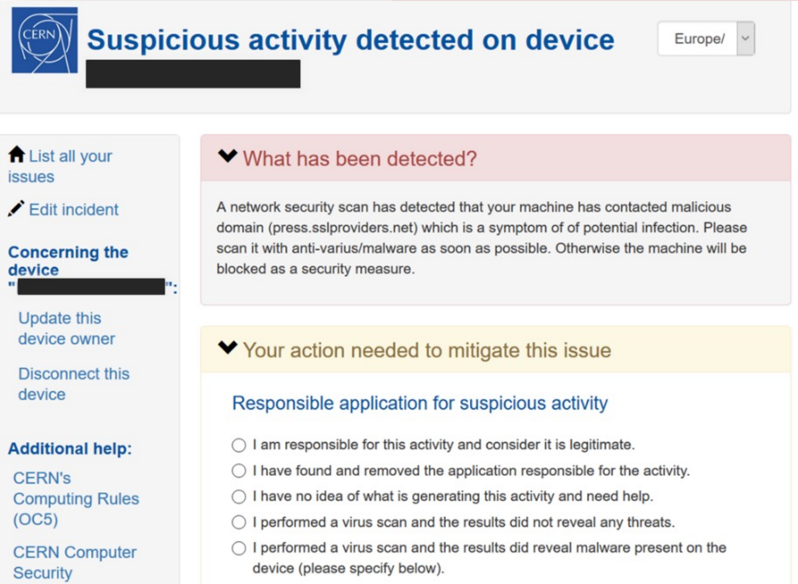
| | |
|---|---|
| Ingesting: | ~3TB of data; |
| Storing currently: | ~220TB in total (~1PB if uncompressed); |
| Analysing per day: | ~3B network connections,<br>~1.2B DNS requests,<br>~570k logins,<br>~4B command executions |

https://home.cern/news/news/computing/computer-security-digital-trenches

**“*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



## Suspicious activity detected on device

[redacted]

List all your issues

Edit incident

**Concerning the device "[redacted]":**

Update this device owner

Disconnect this device

**Additional help:**

CERN's Computing Rules (OC5)

CERN Computer Security

### What has been detected?

A network security scan has detected that your machine has contacted malicious domain (press.sslproviders.net) which is a symptom of of potential infection. Please scan it with anti-varius/malware as soon as possible. Otherwise the machine will be blocked as a security measure.

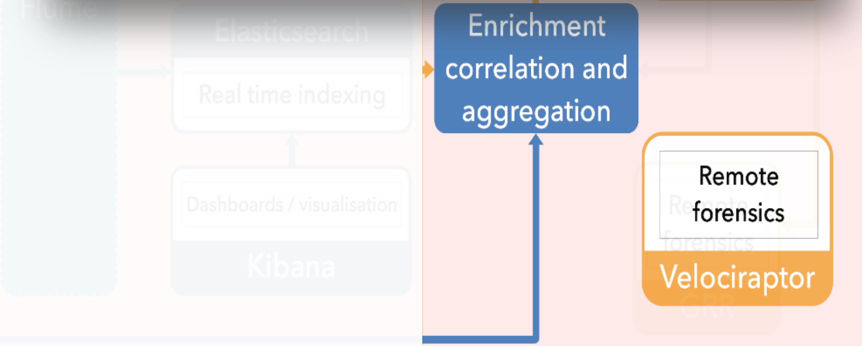
### Your action needed to mitigate this issue

Responsible application for suspicious activity

○ I am responsible for this activity and consider it is legitimate.
○ I have found and removed the application responsible for the activity.
○ I have no idea of what is generating this activity and need help.
○ I performed a virus scan and the results did not reveal any threats.
○ I performed a virus scan and the results did reveal malware present on the device (please specify below).

**Forensics:** Providing capabilities and tools like *Joe Security*, *Prodaft*, *Threatray*, *Velociraptor*.

https://home.cern/news/news/computing/computer-security-catch-me-if-you-can



## CERN Computer Security Rota:

Providing 2nd line "GoD" (with IT), 3rd line "SEC" (with IT-CA), and 4th line Computer Security Officer.

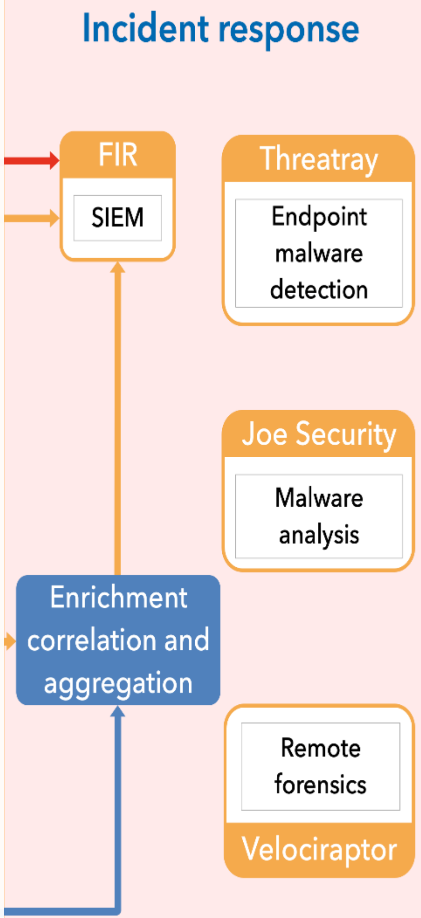
## Grid Security Rota:

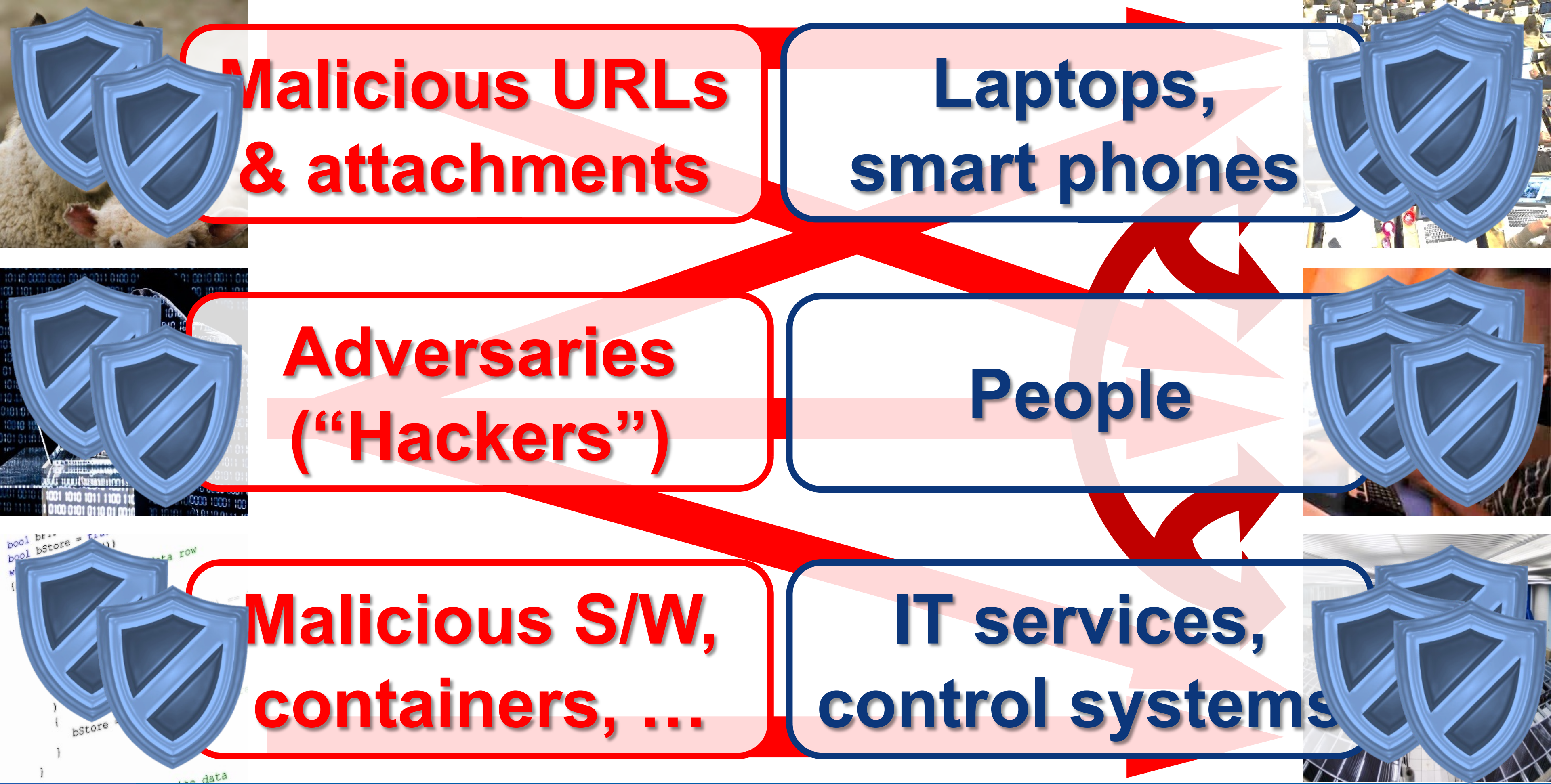
Leading the WLCG Security Office, Leading *EGI* Incident Response Taskforce, Leading *EOSCfuture* Incident Response TF.

## "*SAFER*" Community Security:

Providing world-wide incident response.

https://home.cern/news/news/computing/computer-security-safer-teamwork





Malicious URLs & attachments

Adversaries (“Hackers”)

Malicious S/W, containers, …

Laptops, smart phones

People

IT services, control systems

# Defense in Depth

## “Computer Security” (at CERN) is manyfold and complex.

Still we cover all essential aspects (and hardly cope):

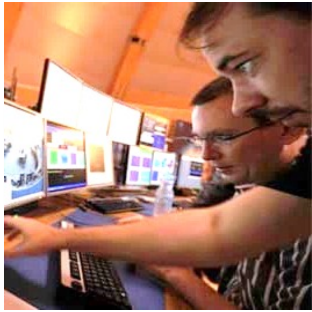
Prevention, Protection, Detection & Response

https://home.cern/news/news/computing/computer-security-permanent-chess

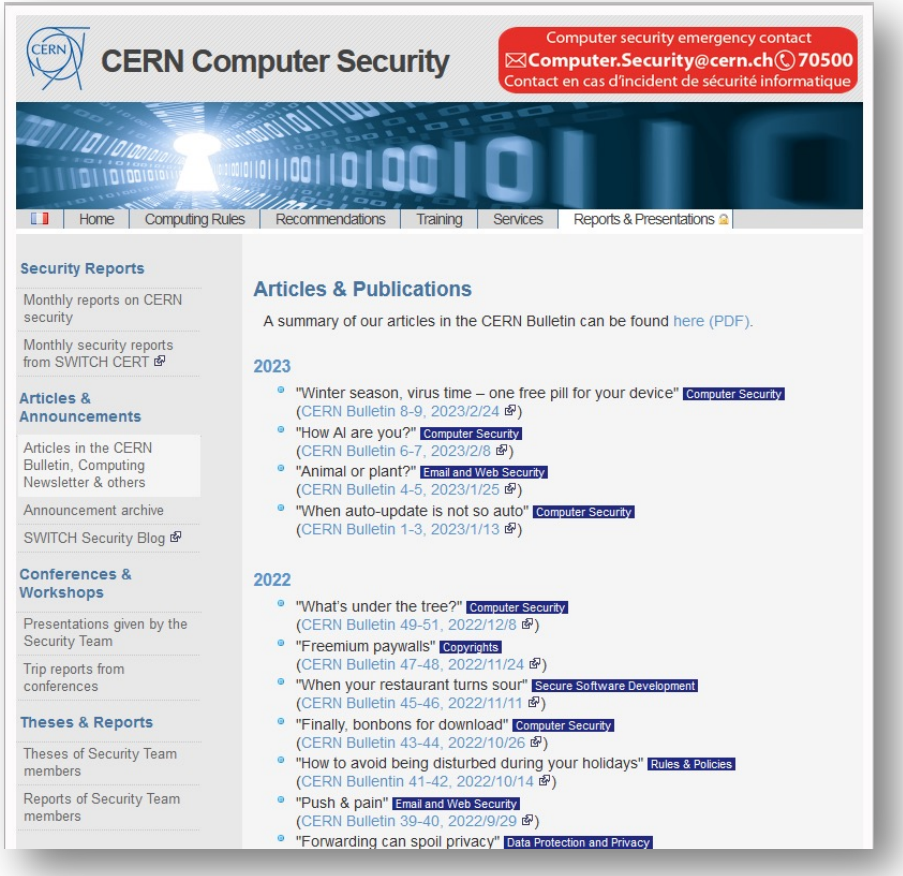
At CERN, *users* are responsible in first instance for the security of their devices, accounts, services(!), data, ...

We try to assist, but need their help and buy-in to ensure your services are secured:

- We discuss new features early
- Design with “security” in mind
- Tackle jointly



# Futher Reading


CERN Computer Security
Computer security emergency contact
Computer.Security@cern.ch 70500
Contact en cas d'incident de sécurité informatique
Home
Computing Rules
Recommendations
Training
Services
Reports & Presentations

**Security Reports**

- Monthly reports on CERN security
- Monthly security reports from SWITCH CERT

**Articles & Announcements**

- Articles in the CERN Bulletin, Computing Newsletter & others
- Announcement archive
- SWITCH Security Blog

**Conferences & Workshops**

- Presentations given by the Security Team
- Trip reports from conferences

**Theses & Reports**

- Theses of Security Team members
- Reports of Security Team members

## Articles & Publications

A summary of our articles in the CERN Bulletin can be found here (PDF).

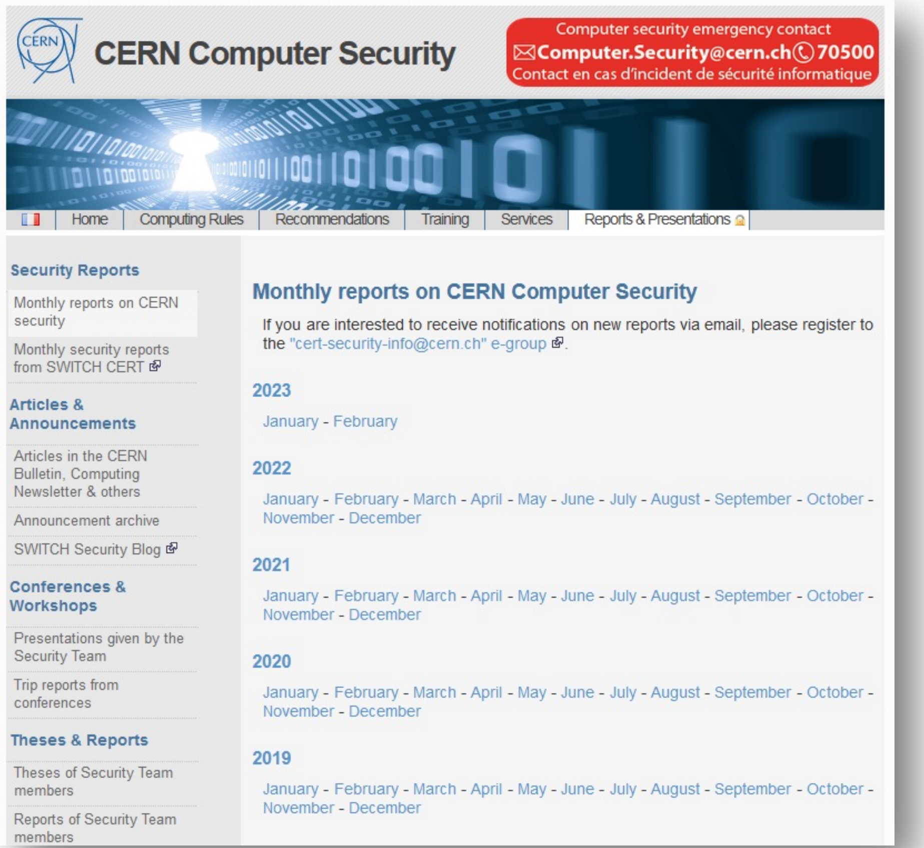
### 2023

- "Winter season, virus time – one free pill for your device" Computer Security (CERN Bulletin 8-9, 2023/2/24)
- "How AI are you?" Computer Security (CERN Bulletin 6-7, 2023/2/8)
- "Animal or plant?" Email and Web Security (CERN Bulletin 4-5, 2023/1/25)
- "When auto-update is not so auto" Computer Security (CERN Bulletin 1-3, 2023/1/13)

### 2022

- "What's under the tree?" Computer Security (CERN Bulletin 49-51, 2022/12/8)
- "Freemium paywalls" Copyrights (CERN Bulletin 47-48, 2022/11/24)
- "When your restaurant turns sour" Secure Software Development (CERN Bulletin 45-46, 2022/11/11)
- "Finally, bonbons for download" Computer Security (CERN Bulletin 43-44, 2022/10/26)
- "How to avoid being disturbed during your holidays" Rules & Policies (CERN Bullentin 41-42, 2022/10/14)
- "Push & pain" Email and Web Security (CERN Bulletin 39-40, 2022/9/29)
- "Forwarding can spoil privacy" Data Protection and Privacy

https://security.web.cern.ch/reports/en/articles.shtml


CERN Computer Security
Computer security emergency contact
Computer.Security@cern.ch 70500
Contact en cas d'incident de sécurité informatique
Home
Computing Rules
Recommendations
Training
Services
Reports & Presentations

**Security Reports**

- Monthly reports on CERN security
- Monthly security reports from SWITCH CERT

**Articles & Announcements**

- Articles in the CERN Bulletin, Computing Newsletter & others
- Announcement archive
- SWITCH Security Blog

**Conferences & Workshops**

- Presentations given by the Security Team
- Trip reports from conferences

**Theses & Reports**

- Theses of Security Team members
- Reports of Security Team members

## Monthly reports on CERN Computer Security

If you are interested to receive notifications on new reports via email, please register to the "cert-security-info@cern.ch" e-group.

### 2023

January - February

### 2022

January - February - March - April - May - June - July - August - September - October - November - December

### 2021

January - February - March - April - May - June - July - August - September - October - November - December

### 2020

January - February - March - April - May - June - July - August - September - October - November - December

### 2019

January - February - March - April - May - June - July - August - September - October - November - December

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