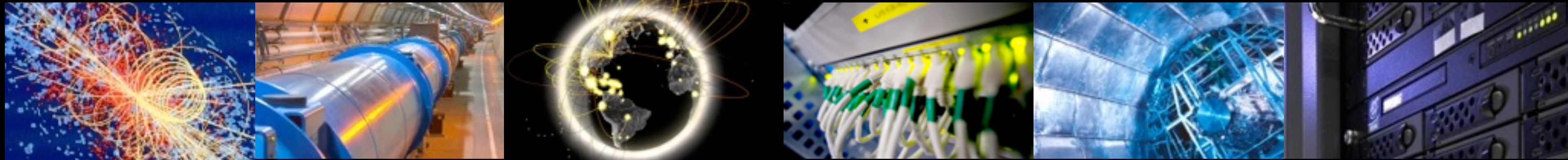


# WLCG Security Operations

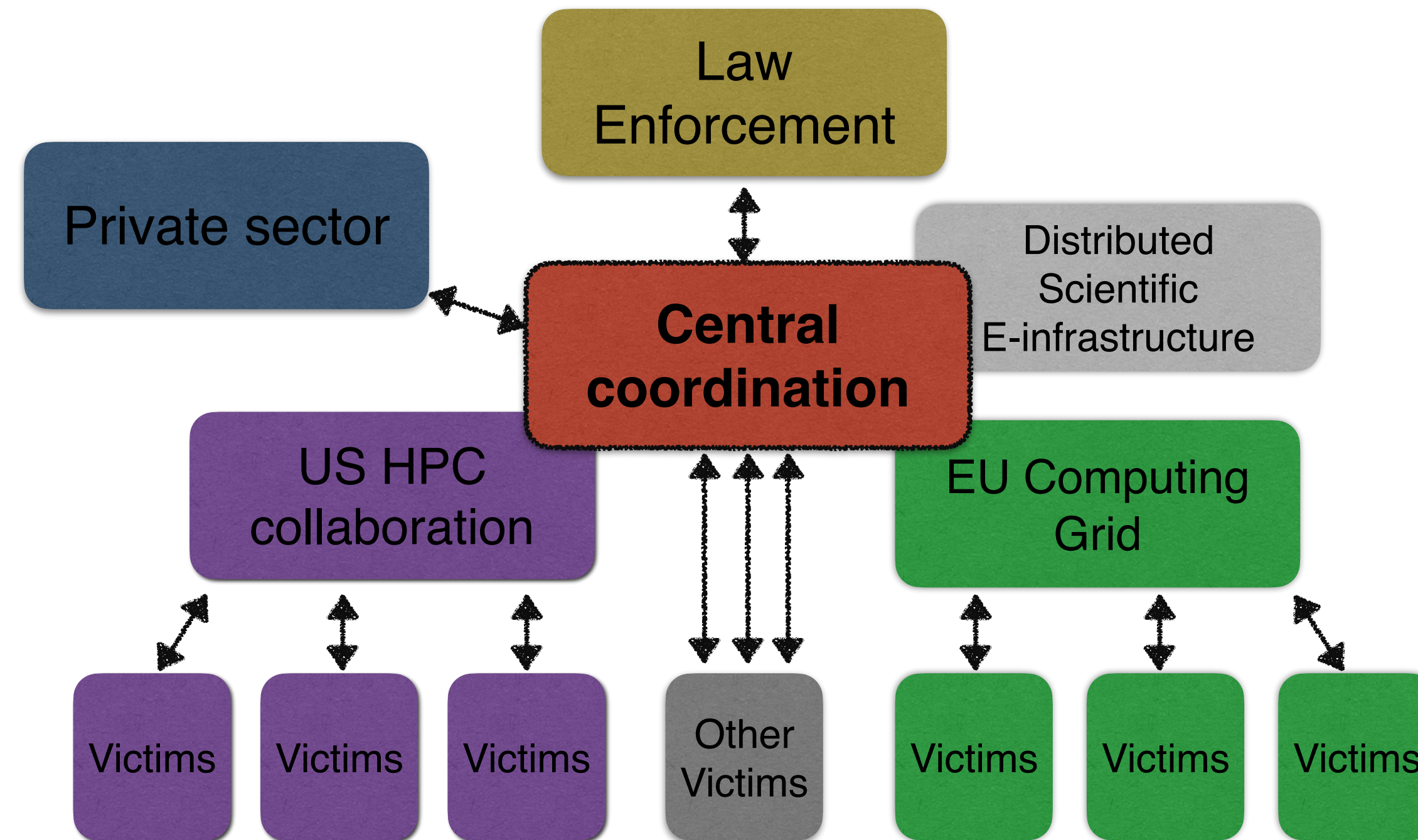
Working with the SAFER trust group &  
recent ransomware attacks

Pau Cutrina (CERN), Tobias Dussa (DFN-CERT), Romain Wartel (CERN)

WLCG Grid Deployment Board, 12th April 2023



# Experience from years of global intrusions



- Ad-hoc team of incident response coordinators
  - Manage and **centralize the information** flow and evidence (may be 1000+ victims)
  - Disseminate the right details to **all potential victims** (direct or via e-infrastructure)
  - **Focus the investigation** on identified goals (key leads)
  - **Mutualize the collective expertise** of involved experts (IOCs, scanner, decryptors)
  - Interface directly with **third parties** (law enforcement)



# Motivation



- Why?

- Defending R&E services and people as a global community
- Concerted and global effort to connect existing groups

- What?

- Systematic, comprehensive, enduring, and truly global incident response and threat intelligence sharing capabilities for the R&E sector as a whole.
- Help to other organisations could take the form of:
  - Sharing threat intelligence to support daily security operations
  - Providing informal emergency incident response assistance
  - Offering members' unique or rare security expertise to support an investigation

# SAFER basics



- Global scope, regardless of country of origin or funding
- Not owned by any entity
- Independent of funding agencies
- As democratic as possible, 100% member-driven
- Self-sustained by contributions from members
- Time, expertise, services, resources, etc.
- Augment – not replace – the capabilities of existing security teams and groups



# Founding members



- + Additional "unlisted" founding members
- 38 members as of March 2023

# SAFER for WLCG



- SAFER is a forum where we can directly interact with:
  - US partners and DoE labs
  - National CERTs
  - Private security vendors
- Ease threat intelligence information sharing
- Additional expertise and skills in case of severe intrusions
- All are the **key aspects of WLCG Security Operations**



# Exposed password notifications

- CERN sources compromised credentials from SAFER and other trust groups
- Clean & filter the data to only keep realistic + “never seen before” passwords
- Leverages a network of security contacts in Research & Education
- Automatically notifies affected organizations
- March 2023: 20 000 passwords sent **per day**.





# Initial Access Brokers

State:  City:  Zip:

ISP:  Outlook:  Per page:  Vendor:

Price:  10 \$

☒ Newest ☐ Older...

Stealer	Country	Links	Outlook	Info	Product	Date	Size	Vendor	Price	Action
Vidar	Zurich ISP: UZH	identity.uzh.ch   connect.uzh.ch   login.teamviewer.com   sdesk.uzh.ch   ipamselfservice.uzh.ch   130.60.88.116   lotus.uzh.ch   zi.uzh.ch   campussoft.uzh.ch   login.aliexpress.com   lasc.uzh.ch   eduid.uzh.ch   130.60.179.71   identity.uzh.ch   connect.uzh.ch   login.teamviewer.com   sdesk.uzh.ch   ipamselfservice.uzh.ch   130.60.88.116   lotus.uzh.ch   zi.uzh.ch   identity.uzh.ch   connect.uzh.ch   login.teamviewer.com   sdesk.uzh.ch   ipamselfservice.uzh.ch   130.60.88.116   lotus.uzh.ch   zi.uzh.ch   identity.uzh.ch   connect.uzh.ch   login.teamviewer.com   sdesk.uzh.ch   ipamselfservice.uzh.ch   130.60.88.116   lotus.uzh.ch   zi.uzh.ch   campussoft.uzh.ch   login.aliexpress.com   lasc.uzh.ch   eduid.uzh.ch   130.60.179.71	-	-	archive.zip	2023.01.18	0.22Mb	Mo####yf [Diamond]	\$ 10.00	<input type="button" value="Buy"/>
Racoon	Solothurn ISP: Finecom Telecommunications AG	symboloo.com   kog.tipp10.com   mega.nz   my.minecraft.net   discordapp.com   accounts.google.com   my.paysafecard.com   streamz.cx   signin.rockstargames.com   marketplace.tracktion.com   Show more...	-	-	archive.zip	2023.01.11	0.23Mb	Mo####yf [Diamond]	\$ 10.00	<input type="button" value="Buy"/>
Racoon	Ticino ISP: M247 Europe	acad-office.com   fashionette.de   brack.ch   unibas.login.eduid.ch   id.mcafee.com   login.live.com   accounts.google.com	-	-	archive.zip	2023.01.09	0.52Mb	Mo####yf [Diamond]	\$ 10.00	<input type="button" value="Buy"/>





# Ransomware

 **swissinfo.ch**

Swiss perspectives in 10 languages

 Sign In

 Search

Science

## Hackers target Zurich university with 'professional' cyberattack


▲ The hack at the University of Zurich is being linked with a spate of cyberattacks on other educational and medical facilities. Keystone / Roland Schlager

The University of Zurich has been hit with a cyberattack that is being linked with a spate of attacks on educational and medical facilities in the region.

February 3, 2023

🕒 2 minutes

[swissinfo.ch/maa](https://www.swissinfo.ch/maa)



techmonitor.ai/technology/cybersecurity/university-of-zurich-cyb

All Sections

Cybersecurity

Digital economy

Hardware

Leadership

Government


TECHNOLOGY > CYBERSECURITY


February 3, 2023


## University of Zurich hit with 'serious' cyberattack


The attack on Switzerland's largest university is the latest in a line of hacks on German-language speaking institutions.

By Ryan Morrison










The University of Zurich has become the latest in a long line of German-language institutions to be hit by a [cyberattack](#) in recent weeks. The university says it isn't aware of any data being encrypted or extracted and IT services are continuing to operate as normal following the attack, which took the university's website offline earlier today.







# Ransomware

[Home](#) > [News](#) > [Security](#) > Vice Society ransomware leaks University of Duisburg-Essen's data

## Vice Society ransomware leaks University of Duisburg-Essen's data

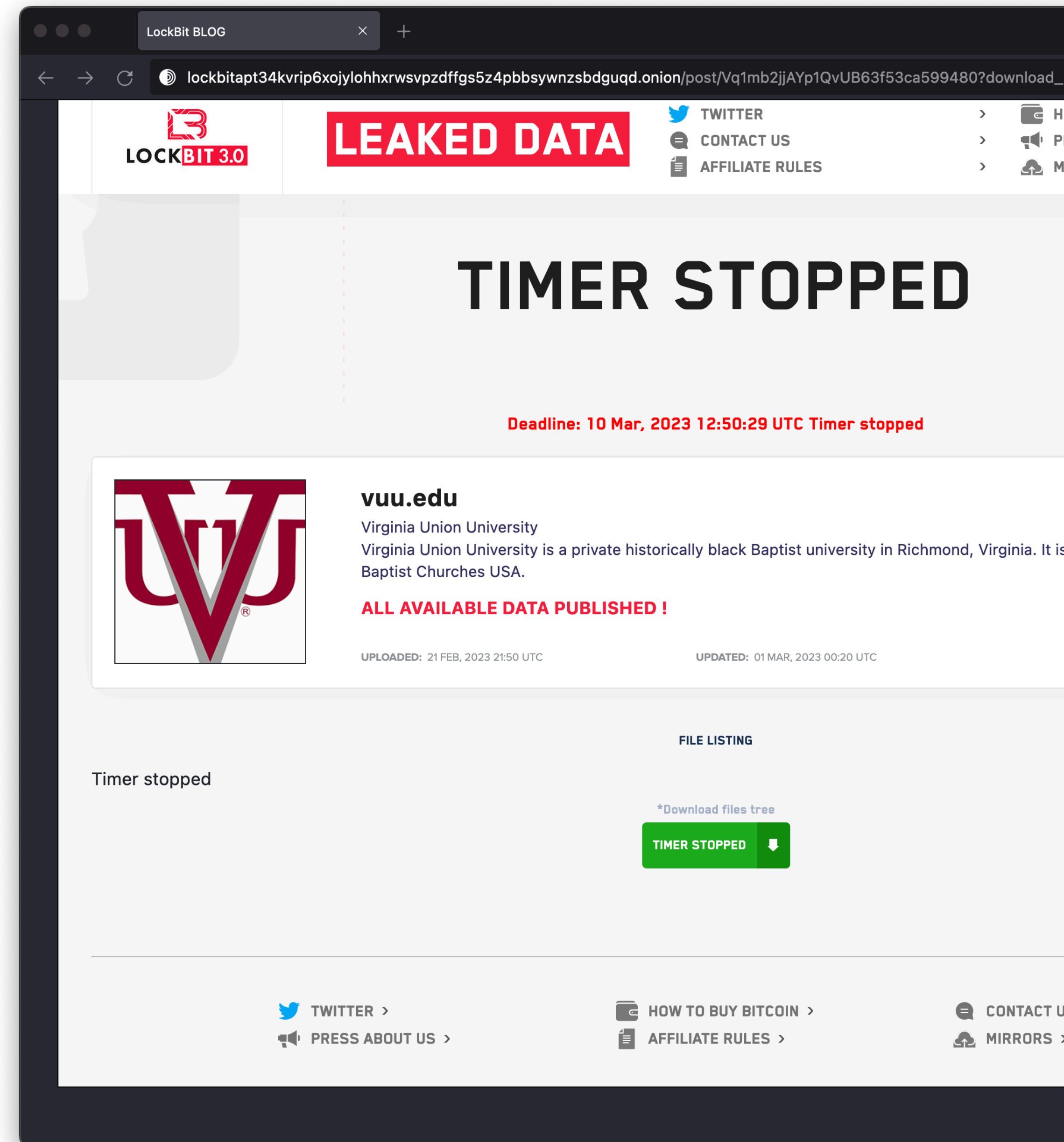
By [Bill Toulas](#)

January 16, 2023 02:22 PM 0



The Vice Society ransomware gang has claimed responsibility for a November 2022 cyberattack on the University of Duisburg-Essen (UDE) that forced the university to reconstruct its IT infrastructure, a process that's still ongoing.

The threat actors have also leaked files they claim to have stolen from the university during the network







# Ransomware



arstechnica.com/information-technology/2022/10/how-vice-



BIZ & IT

TECH

SCIENCE

POLICY

CARS

GAMING & CULTURE

STORE

FORUMS

SUBSCRIBE



SIGN IN

EXTREMELY AVERAGE —

## How Vice Society got away with a global ransomware spree

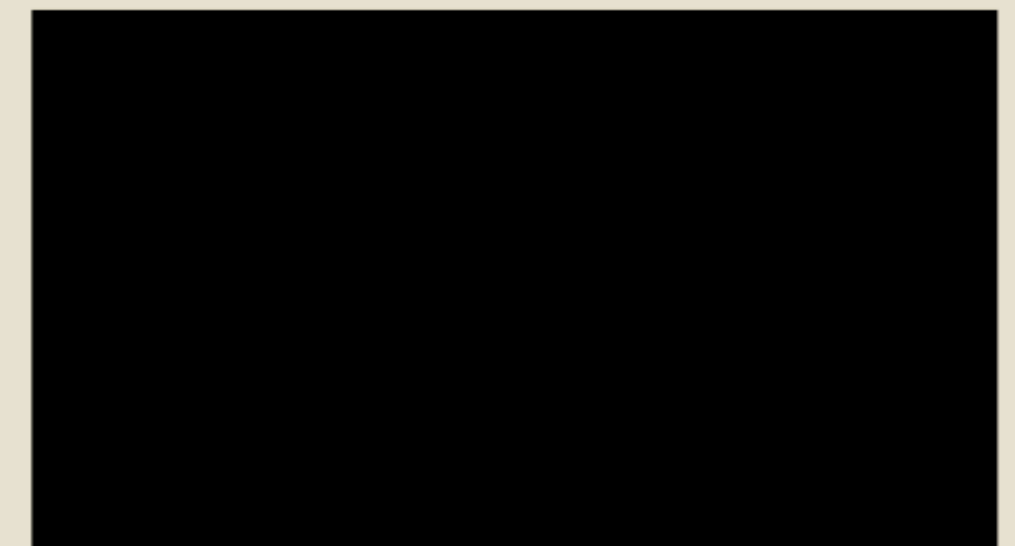
Vice Society has a superpower that's allowed it to quietly thrive: Mediocrity

LILY HAY NEWMAN, WIRED.COM - 10/21/2022, 3:24 PM



ARS VIDEO

How The Callisto Protocol's Gameplay Was Perfected Months Before Release







# Responding to ransomware attacks

- Via SAFER/WLCG/CERN, an informal cooperation with Prodaft started in Q4 22
- Prodaft consistently provided high quality targeted threat intel
- SAFER/WLCG/CERN:
  - Identified trusted security contact points at affected organizations
  - Passed-on the information from Prodaft for immediate action and remediation
  - Shared back with Prodaft additional indicators or relevant feedback (when possible)
- One of the most impactful security cooperations in the last decade for WLCG
  - We could directly intervene at victim organizations just **before** ransomware deployment
  - Major **impact averted at dozens of Research & Education organizations** worldwide  
*...in Australia, Austria, Canada, Denmark, Germany, Greece, Hong Kong, Japan, Iceland, Italy, Switzerland, Taiwan, the UK and the US — many affiliated with WLCG or part of our academic community.*



# Responding to ransomware attacks

- Collaboration needs to be mutually beneficial:
  - *"We tried many different ways of informing victims. However, cooperation with SAFER/WLCG/CERN has proven to be the most effective and rapid way of stopping these incidents. Detecting threats before the attack is crucial, but it does not mean anything unless you have a responsive partner that can disseminate this to victims globally in a timely manner."* – Prodaft.
- Trying to position SAFER as a global, unique entry point for security vendors
  - Requires significant efforts to reach out and follow up with affected R&E organizations
  - However:
    - Reinforces connections with the community
    - Beneficial and attractive "easy" contact point for R&E for security vendors
    - Access to invaluable intel
  - Discussions started with additional possible partners





# Example of response in DFN-CERT

- Constituency: On the order of several hundred academic orgs in Germany
  - Including EGI sites
  - DFN-CERT is actively contributing to the EGI-CSIRT
- Alerts for 20+ infections received through SAFER ... in the past three months!
- No false positives that we are aware of
- Some extremely high-profile cases
- Some victims informed in time to keep the baddies out





## AFFILIATE PROGRAM

The Black Hole Locker affiliate program welcomes you. As a company created by former [REDACTED] security experts, we believe strongly that trust is earned through transparency.

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.

**Tuesday 14th February 14:00, IT Auditorium**

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

Pushing the boundaries of ransomware!

If you have questions, please contact us:

[blackholelocker@reallyfast.biz](mailto:blackholelocker@reallyfast.biz)

**we are hiring!**

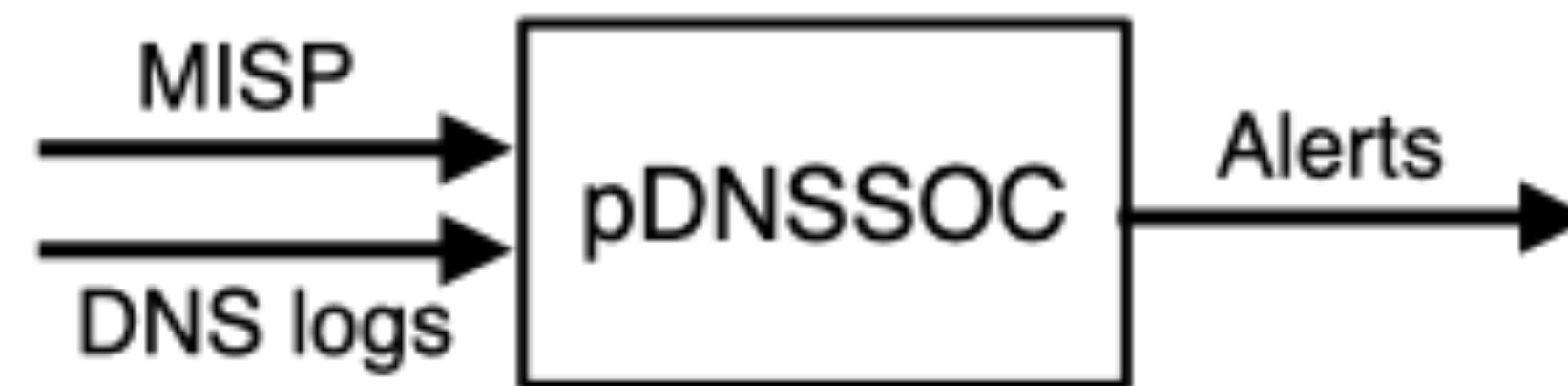






# pDNSSOC

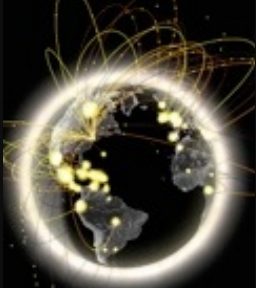
- Correlating DNS logs with threat intel from MISP as a poor man's SOC
    - pDNSSOC provides a turn-key solution to detect and respond to security incidents
  - The basics:
    - Designed for central security teams to support smaller entities (typically with less time/manpower/expertise/tools for security) in their circle of actions.
    - Get the local admins to send you DNS logs or privacy-preserving pDNS data, and **pDNSSOC correlates this with suspicious/malicious domains**, synced from one or more MISP instances the central security team has access to.
- Deployment takes < 10 sec (+ 1 configuration file for MISP details & email alerts).



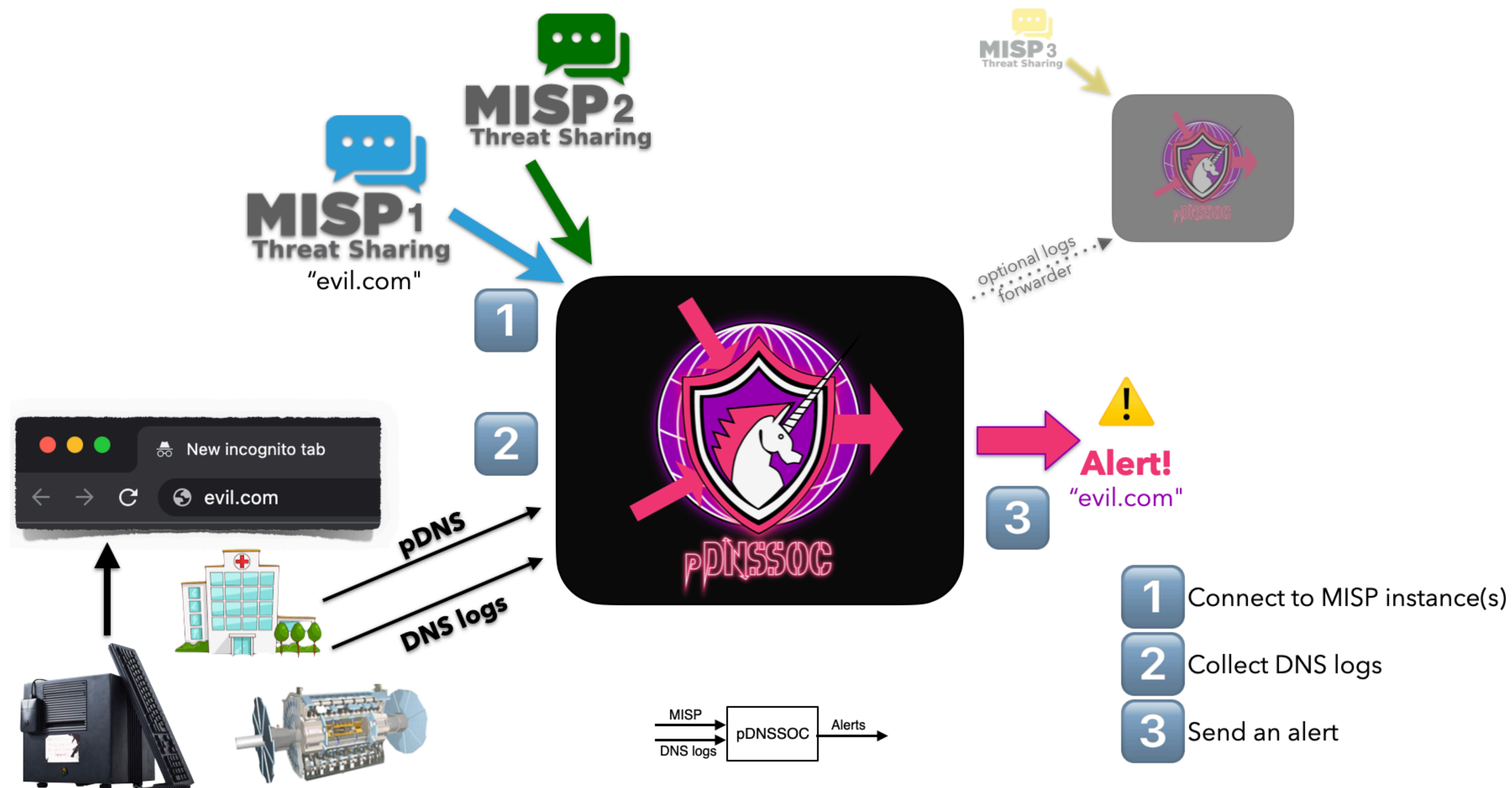
<https://github.com/CERN-CERT/pDNSSOC>







# pDNSSOC





# pDNSSOC

Home

Event Actions

Dashboard

Galaxies

Input Filters

Global Actions

Sync Actions

Administration

Logs

API

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Add Event Report

Populate from...

Enrich Event

Merge attributes from...

Propose Attribute

Propose Attachment

Publish Sightings

Download as...

NCSC-NL

[OSINT] Talos uncovers espionage...

Event ID

41518

UUID

f88f5058-019f-4e02-bb83-dc0f02390a73

Source Organisation

NCSC-NL

Member Organisation

WLCG

Creator user

liviu.valsan@cern.ch

Tags

tlp:white

ncsc-nl-ndn:feed="generic"

Date

2023-03-15

Threat Level

Medium

Analysis

Ongoing

Distribution

All communities

Info

[OSINT] Talos uncovers espionage campaigns





19



# pDNSSOC

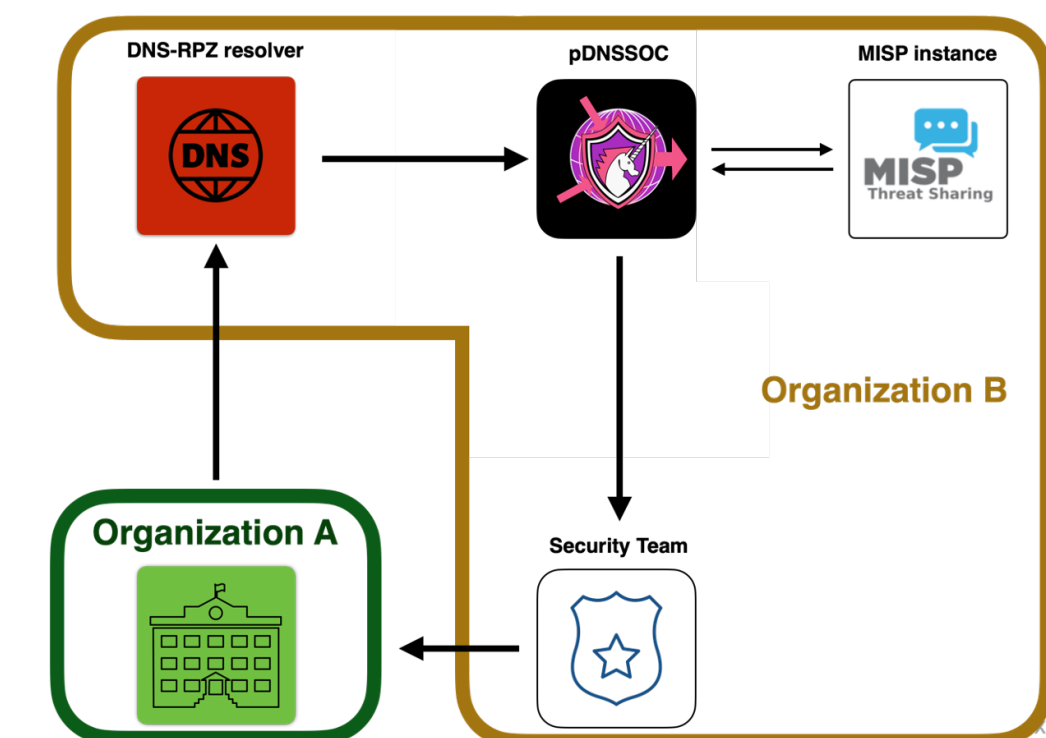
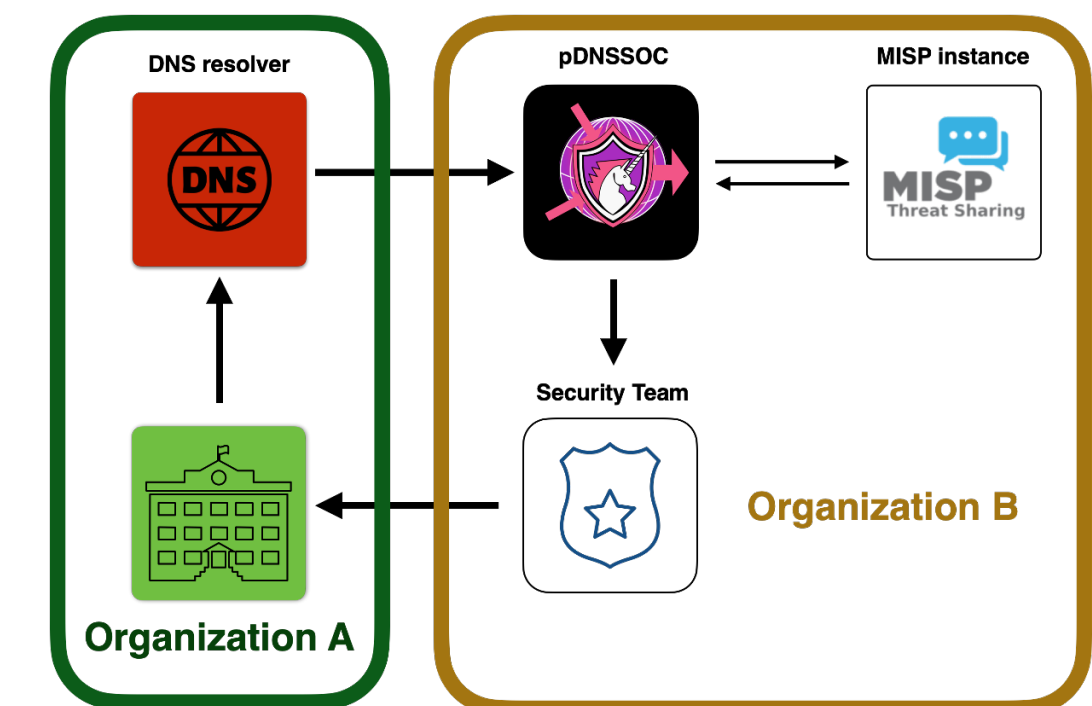
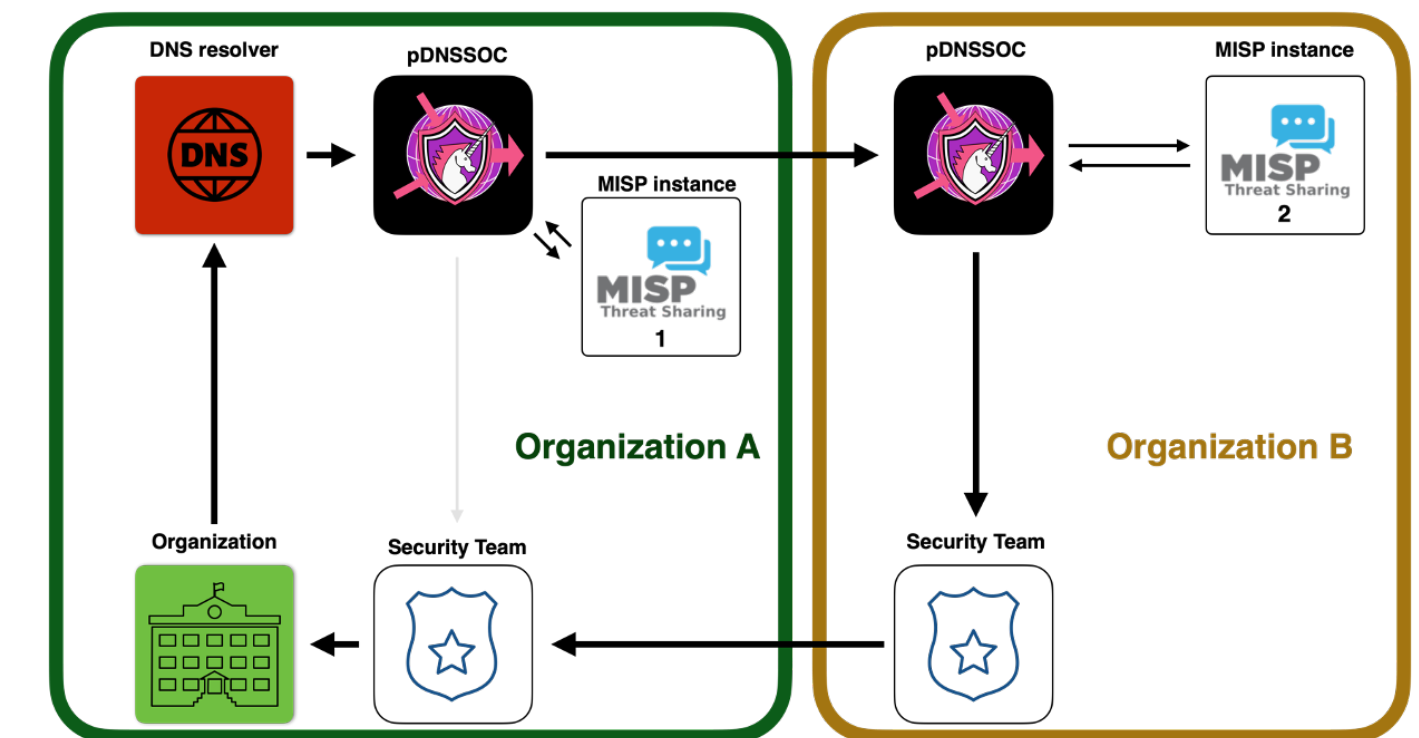
<div><div></div><div>pdnssoc-dev@cern.ch</div><div>[pDNSSOC] Swiss Health organizations alert</div><div>To: Romain Wartel</div></div> <div>Inbox - CERN Yesterday at 23:18</div>								
pDNSSOC client	First Occurrence	Malicious domain	MISP event	Total # of IoCs	Publication	Organisation	Comment	Tags
188.184.75.204	07-Dec-2022 07:11:17.403	nnpcoil.buzz	<a href="#">AZORult Spam Run (2022-02-22 - Inquiry: Modez Professional Systems RFQ)</a>	24	2022-02-22	GovCERT	C&C	
188.184.75.204	07-Dec-2022 07:11:21.601	<a href="#">dgsheohong.com</a>	<a href="#">AgentTesla Spam Run (2022-02-22 - Re: Revised PO - Items 22940)</a>	25	2022-02-22	GovCERT	C&C	
188.184.75.204	07-Dec-2022 07:11:26.550	ekens.top	<a href="#">Lokibot Spam Run (2022-10-19 - Unknown)</a>	13	2022-10-19	GovCERT	C&C	nukify-botnet-domain-bad
			<a href="#">Lokibot Spam Run (2022-11-04 - Due Date For Latest Remittance)</a>	31	2022-11-04	GovCERT	C&C	nukify-botnet-domain-bad
188.184.75.204	07-Dec-2022 07:11:30.423	kizitox.cf	<a href="#">AgentTesla Spam Run (2022-02-15 - product inquiry)</a>	24	2022-02-15	GovCERT	exe.dropper	
			<a href="#">AZORult Spam Run (2022-02-22 - Inquiry: Modez Professional Systems RFQ)</a>	24	2022-02-22	GovCERT	exe.dropper	



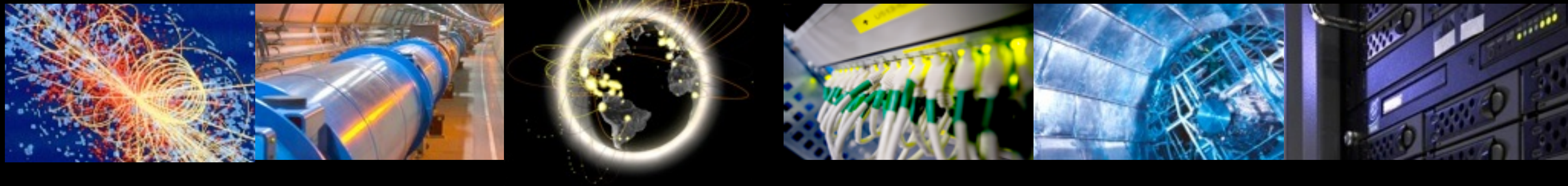


# Different pDNSSOC setups

- Federation:
  - The organization forwards pDNS data using a **pDNSSOC forwarder**.
  - You can detect the intrusion at different levels while respecting the TLP.
- Collaboration:
  - The organization **forwards DNS/pDNS logs**.
  - You cannot block the requests but you get the alerts.
- Responsive:
  - The organization use your DNS resolver.
  - You host the **DNS + RPZ** (you can block requests) and pDNSSOC (you get the alerts).



# Demo







# How can you use it?

- If you want to operate a pDNSSOC server:
  - Download + deploy <https://github.com/CERN-CERT/pDNSSOC>
  - Connect to the CERN MISP instance
  - Collect DNS data from your community/sites/hosts/constituency
  - Contact [wlcg-security-officer@cern.ch](mailto:wlcg-security-officer@cern.ch) to explore nesting with other pDNSSOC instances
- If you are a site with very limited security expertise/effort and no active SOC
  - Explore how you can collect/send DNS logs or privacy-preserving pDNS data
    - No recompilation of BIND, no installation of extra packages
    - Configuration on the client must be doable in < 5 min
  - Contact [wlcg-security-officer@cern.ch](mailto:wlcg-security-officer@cern.ch) to identify a suitable pDNSSOC instance



# Questions / Discussion

