



**DNS4EU**

**a part of Europe's cyber  
defense and cyber  
resilience strategy**

Adam Měrka | Technical consultant

Project number: 101095329 21-EU-DIG-EU-DNS  
Project name: DNS4EU and European DNS Shield.  
This project is co-funded by the European Union.



Co-funded by  
the European Union

# Agenda

1. What is Protective DNS?
2. The DNS4EU Project
3. Threat Intelligence
4. Real-life examples
5. Challenges
6. Q&A

# DNS n Cybersecurity



**15B**  
connected devices



**94%**  
of attacks rely on DNS

# The rise of Protective DNS (PDNS)



# DNS4EU project



Co-funded by  
the European Union

# DNS4EU

= safe, stable and private  
internet for Europe

## Goal of ENISA

Strengthen the digital security and independence of the European Union.

## Challenge

EU governmental institutions and citizens are not well protected with slow reaction on threats. Protections on DNS level are not located in EU.

## Solution

Create an independent EU-based DNS protection with real-time reaction on threats with easy distribution to the citizens and institutions.



# DNS4EU Consortium





Project Leader

 Whalebone, s.r.o.

## Consortium members

-  CZ.NIC
-  Czech Technical University Prague
-  Time.lex
-  deSEC
-  Sztaki
-  ABI Lab Centro di Ricerca e Innovazione per la Banca
-  Naukowa i Akademicka Sieć Komputerowa
-  Directoratul Național de Securitate Cibernetică

## Associated partners

-  Ministry of Electronic Governance
-  CESNET
-  F-Secure
-  Centro Nacional de Cibersegurança

A background image of space showing the Earth's horizon. The sky is a deep blue, transitioning to a lighter blue near the horizon. A bright comet with a long tail is visible in the upper left. The sun is visible on the right side of the horizon, creating a bright glow.

# Threat intelligence



# Basic Pillars



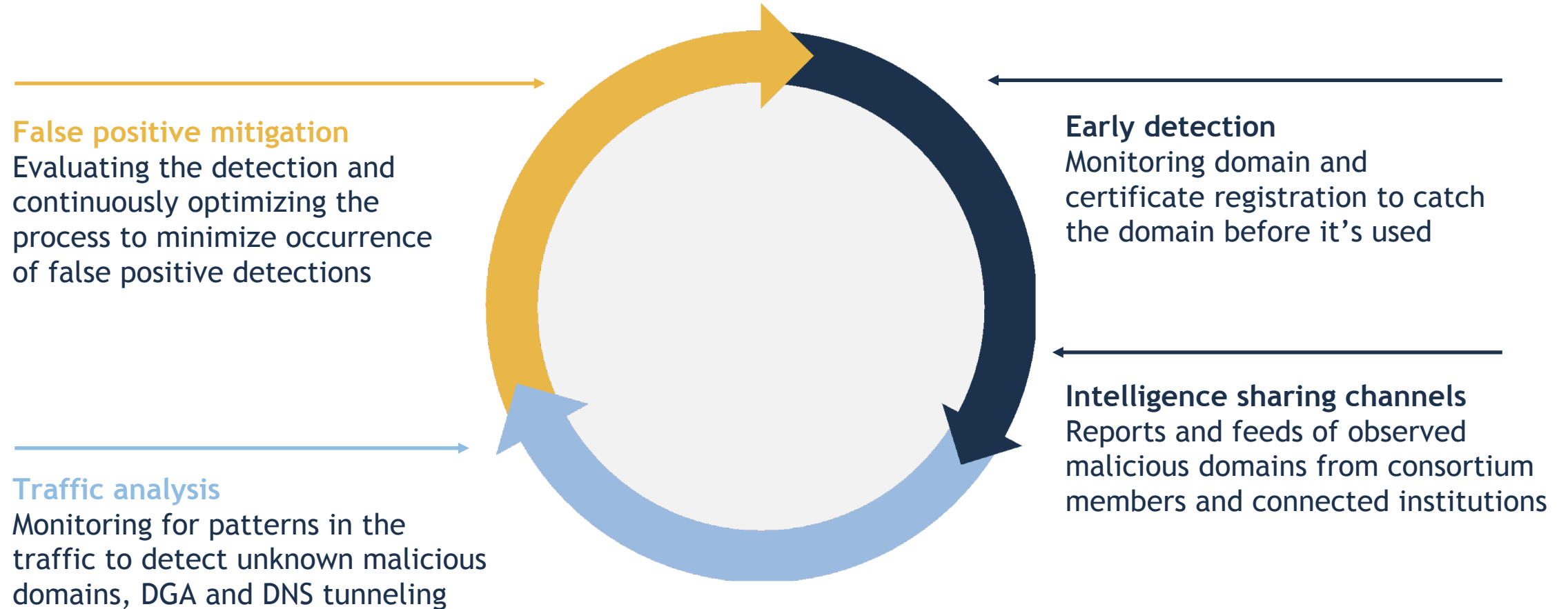
## Input

Threat intelligence data from dozens of Telco operators

## Output

Protection of millions of users and organisations (Bank's clients)

# Threat Intelligence lifecycle



# Threat intelligence sharing

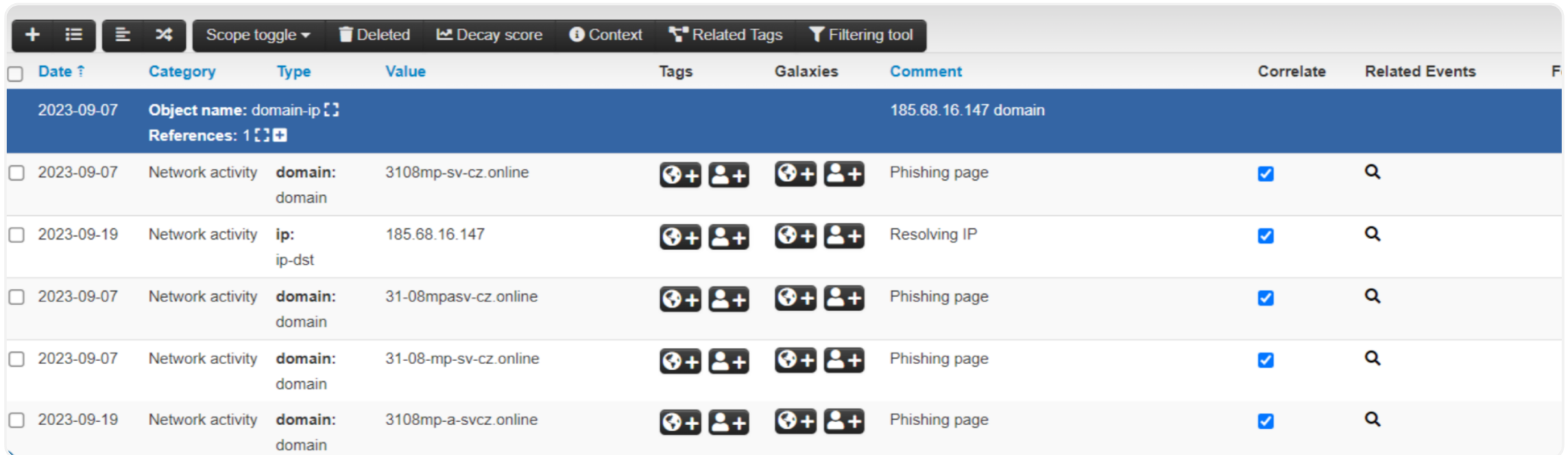
Sharing is caring!



- DNS4EU provides central place to block DNS threats for millions of people
- Easy and automated connection
- Public & Private sector

# Regional Threat Intelligence (MISP)

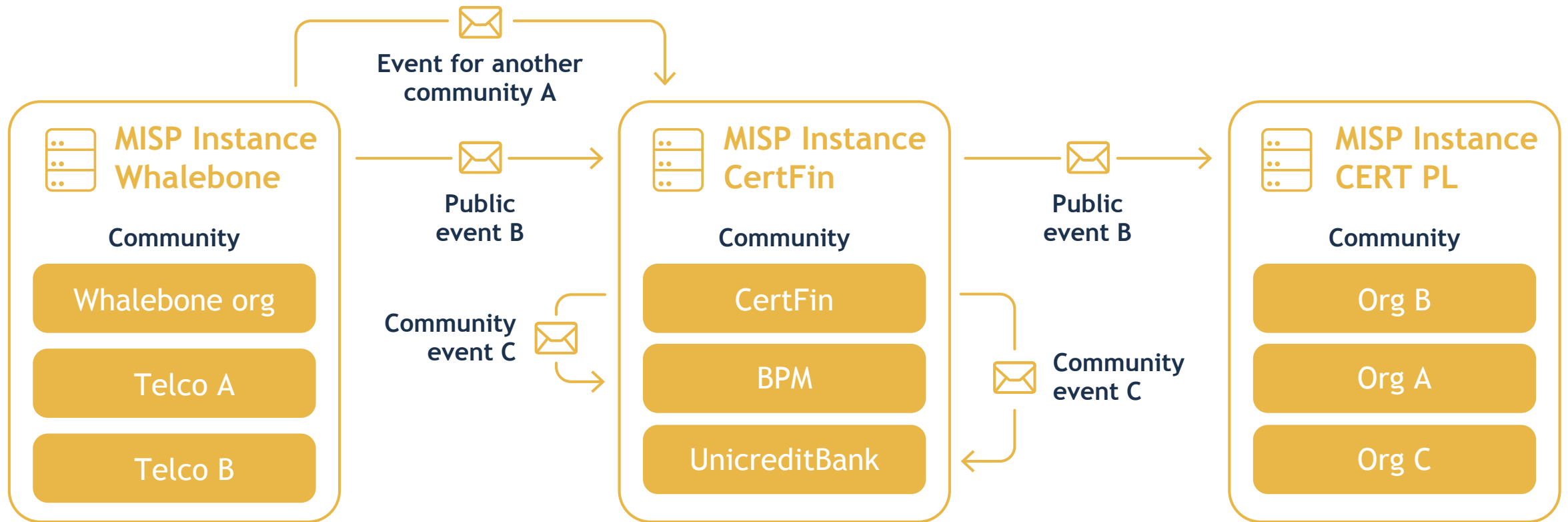
- Open-source Threat Intelligence and sharing platform
- Distributed servers which can create, consume or forward TI data about malicious domains, IPs and more
  - Any CERT, CSIRT or commercial subject can run their own instance and/or connect to the DNS4EU instance
- Allow to enter many types of threats with context, tags, commentary and more



The screenshot displays the MISP web interface. At the top, there is a navigation bar with icons for home, search, and other functions, along with a search bar and several filter buttons: 'Scope toggle', 'Deleted', 'Decay score', 'Context', 'Related Tags', and 'Filtering tool'. Below the navigation bar is a table with the following columns: 'Date', 'Category', 'Type', 'Value', 'Tags', 'Galaxies', 'Comment', 'Correlate', and 'Related Events'. The table contains several rows of data, including a summary row for a domain-ip and several individual network activity entries. Each entry includes a date, category, type, value, tags, galaxies, comment, and correlation status.

Date	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
2023-09-07	Object name: domain-ip References: 1					185.68.16.147 domain		
2023-09-07	Network activity	domain: domain	3108mp-sv-cz.online			Phishing page	<input checked="" type="checkbox"/>	
2023-09-19	Network activity	ip: ip-dst	185.68.16.147			Resolving IP	<input checked="" type="checkbox"/>	
2023-09-07	Network activity	domain: domain	31-08mpasv-cz.online			Phishing page	<input checked="" type="checkbox"/>	
2023-09-07	Network activity	domain: domain	31-08-mp-sv-cz.online			Phishing page	<input checked="" type="checkbox"/>	
2023-09-19	Network activity	domain: domain	3108mp-a-svcz.online			Phishing page	<input checked="" type="checkbox"/>	

# Regional Threat Intelligence (MISP)



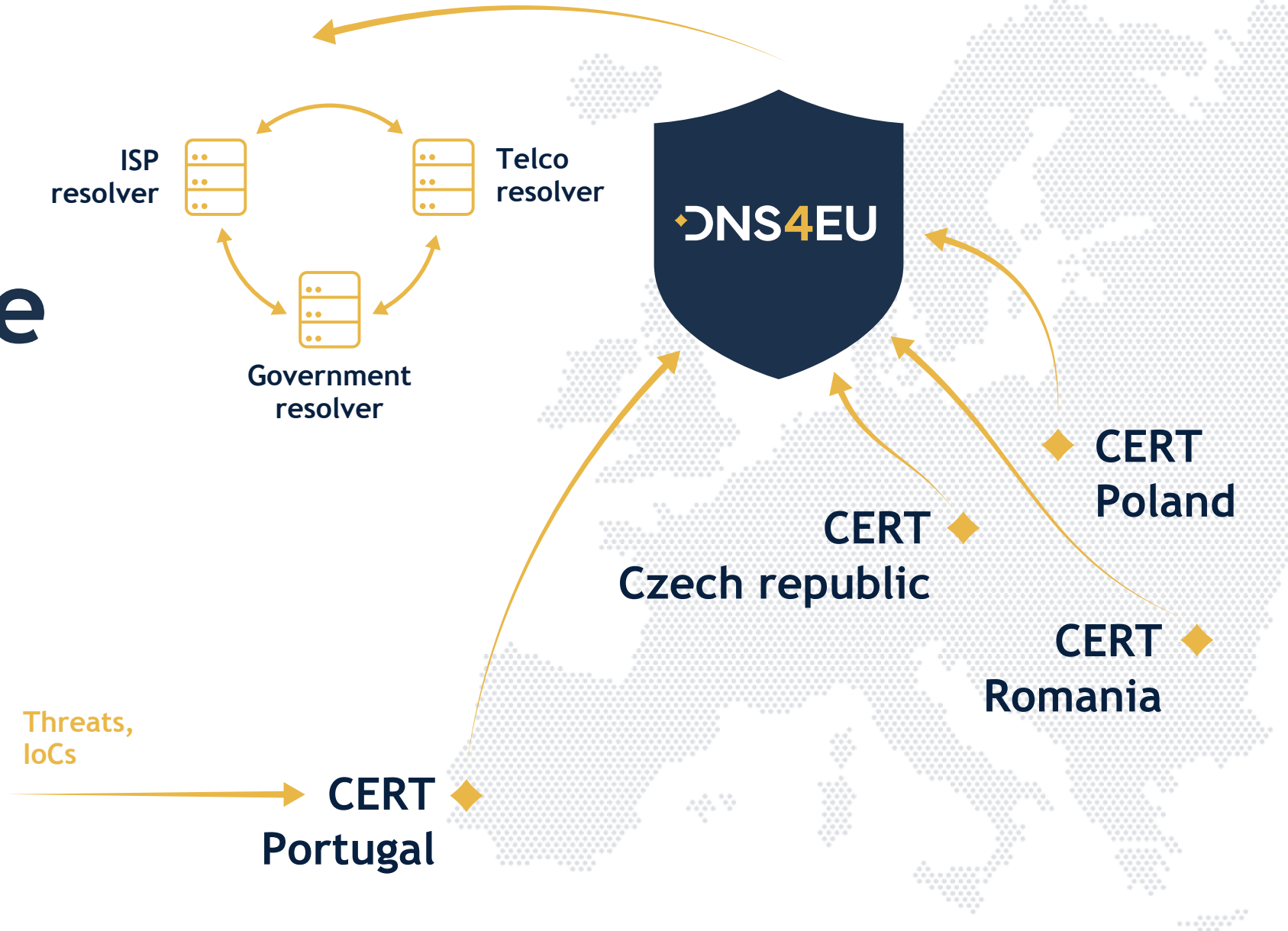
# Connected institutions, quick stats

- 4 CERTs already connected, others currently integrating
- 179,527 events total
- 597 remote organizations connected
  - 16 banks, one from italy
- 

ID	Name	UUID	Description	Nationality	Sector	Type
596	CERT EE	b18c9ace-982c-4648-ba3c-9792346ab7d3		 Estonia	CERT	CERT Estonia
595	CERT Fin	4c18fe58-00dd-4229-9c0f-a20b397a8abb		 Italy	Private	ISAC
137	CERT-RO	5c35d621-4a34-4dd7-8a59-6f0f6c197fc2	Directoratul Național de Securitate Cibernetică (DNSC)	 Romania	Government	CERT-RO
1	DNS4EU	7a6689d5-5231-4258-a7af-3036714ac421				ADMIN
3	External-test	debeceb7-6464-465a-9726-e672e2443b44		 Czechia		
138	HUN-CERT	f2128a5f-e9d5-4b8a-a925-059160b0f9c5	Institute for Computer Science and Control - Sztaki	 Hungary	Government	HUN-CERT
135	O2 Czech republic	dff566ac-dd53-4a82-981f-6181e1ee23e2		 Czechia	Telco	
594	Telecom Liechtenstein	f307a297-b1cd-4b44-a8cb-54b12c60a2ab		 Liechtenstein	Telco	Telco
2	Whalebone	79626308-f35a-4e68-80c4-35d18dd4580b		 Czechia		

# Regional Threat Intelligence

-  Banks
-  Ministry of social affairs
-  Parcel delivery service
-  Information Sharing & Analysis Centre
-  Postal Service



A background image of space showing the Earth's horizon with a blue and orange glow, a bright comet streak in the upper left, and a bright sun or star on the right horizon.

# Real-life **examples**



# Real-life example: Luxembourg

## Fake Post Courier (post-client-lu.com)

SMS  
E-mail

Personal  
information

The screenshot shows a mobile application interface for 'Post'. At the top, there is a logo and the text 'Confirmez vos informations de facturation'. Below this, there are several input fields: 'Nom', 'Prénom', 'Date de naissance', 'Numéro de téléphone', 'Adresse', 'Ville', and 'Code postal'. At the bottom, there is a yellow button labeled 'Continuer'.

Credit  
card

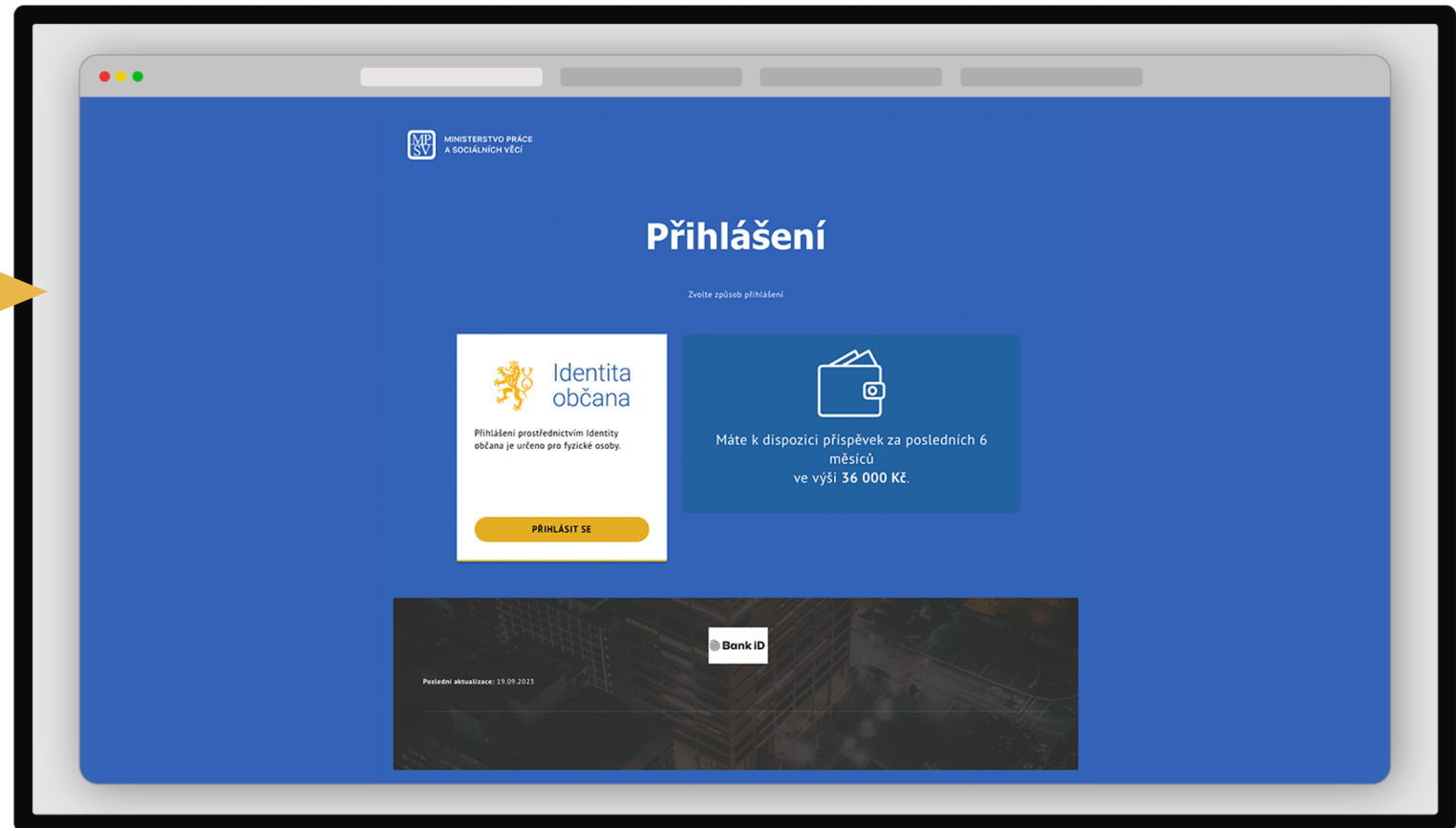
The screenshot shows a mobile application interface for 'Post'. At the top, there is a logo and the text 'Paiement des frais supplémentaires' and 'Montant : 0.48€'. Below this, there are logos for 'VISA' and 'MasterCard'. There are four input fields: 'Nom sur la carte', 'Numéro de carte', 'Expiration MM/AA', and 'Cryptogramme (CVV)'. At the bottom, there is a yellow button labeled 'Continuer'.

# Real-life example: Czech Republic

## Fake Ministry of Social Affairs (npsv.online)

SMS

Login  
to internet  
banking



# EU-wide examples

## Fake fines from the ministry of finance (clones)



Sie haben einen ausstehenden Betrag mit dem Aktenzeichen 23894891 auch nach mehreren Mahnungen nicht bezahlt. Am 2. Marsch 2023 wird der Gerichtsvollzieher Ihren Hausrat vorläufig pfänden. Sie können die Pfändung abwenden, indem Sie den vollen Betrag sofort bezahlen mit **echtzeit überweisung**.

**JETZT BEZAHLEN**

Beschreibung	Betrag	Begünstigter	Status	Gesamt
Laufende Nummer: 23894891	€349	Bundesministerium für Finanzen	Läuft heute ab	€349
<b>Zwischensumme</b>				<b>€349</b>
<b>Gesamtsumme</b>				<b>€349</b>

ACHTUNG! In dem zu zahlenden Betrag sind keine Rückforderungszinsen enthalten. Der derzeitige jährliche Zinssatz beträgt 0,01 %. Der zu zahlende Betrag und etwaige Verzugszinsen müssen innerhalb von 24 Stunden nach dem Datum dieser Mahnung auf dem Konto der Steuerbehörde eingegangen sein. Wenn Sie nicht fristgerecht zahlen, werden weitere Inkassomaßnahmen eingeleitet.

Print

Download

gov.pl | Serwis Rzeczypospolitej Polskiej

Strona główna  
Rada Ministrów  
Kancelaria Premiera  
Ministerstwa  
Urzędy, instytucje i placówki RP

Usługi dla obywatela  
Usługi dla przedsiębiorcy  
Usługi dla urzędnika  
Usługi dla rolnika

Koronawirus: informacje i zalecenia  
Zalóż Profil zaufany  
Baza wiedzy  
Serwis Służby Cywilnej

Сайт для громадян України – Serwis dla obywateli Ukrainy

### Odszkodowanie 2022

Andrzej Duda i Unia Europejska podpisali dekret przyznający specjalne odszkodowania dla wszystkich mieszkańców Polski. Wysokość swojego odszkodowania możesz sprawdzić za pośrednictwem naszego serwisu. Maksymalna kwota odszkodowania wynosi 5 000 euro. Aby sprawdzić - kliknij na poniższy przycisk.

**CHCIAŁABYM WIEDZIEĆ**

**Kto jest uprawniony do otrzymania odszkodowania?**

**Ile razy można go dostać?**

**Gdzie pójść te pieniądze?**

Ostatnia aktualizacja: 03.12.2022 16:14  
Instytucja odpowiedzialna za usługę: Ministerstwo Cyfryzacji

Polityka cookies | Służba cywilna | Profil zaufany | BIP | Prawa autorskie  
Warunki korzystania | Geoportal | Deklaracja dostępności serwisu Gov.pl

Strony dostępne w domenie www.gov.pl mogą zawierać adresy skrzynek mailowych. Użytkownik korzystający z adresu będącego adresem e-mail dobrowolnie podanych danych w wiadomości w celu przesłania odpowiedzi na przesłane pytania. Szczegóły przetwarzania danych przez każdą z jednostek osobowych.

Wszystkie treści publikowane w serwisie są udostępniane na licencji Creative Commons: uznanie autorstwa - użycie niekomercyjne - bez utworów zależnych 3.0 Polska (CC BY-NC-ND 3.0 PL), o ile nie jest to stwierdzone inaczej.

Fundusze Europejskie Polska Cyfrowa | Rzeczypospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

W celu świadczenia usług na najwyższym poziomie stosujemy pliki cookies. Korzystanie z naszej witryny oznacza, że będą one zainstalowane w Twojej przeglądarce. W każdym momencie możesz dokonać zmiany ustawień Twojej przeglądarki. [Zobacz politykę cookies.](#)

Belastingdienst

U heeft een openstaande bedrag met het kenmerk: BS83289982 na meerdere herinneringen niet voldaan. Op 11 jan 2023 zal de gerechtsdeurwaarder overgaan tot conservatoir beslag op uw inboedel. U kunt de beslagprocedure voorkomen door direct het gehele bedrag te voldoen via IDEAL.

**NU BETALEN**

Omschrijving	Bedrag	Begunstigde	Status	Total
Kenmerk: BS83289982	€289	Federale Overheidsdienst Financien	Verloopt vandaag	€289
<b>Subtotaal</b>				<b>€289</b>
<b>Totaal</b>				<b>€289</b>

Let op! In het te betalen bedrag is geen invorderingsrente opgenomen. Het huidige rentepercentage op jaarbasis is 0,01%. Het te betalen bedrag en de eventuele invorderingsrente moeten binnen 24 uur na het dagtekening van deze aanmaning op de rekening van de Belastingdienst staan. Als u niet op tijd betaald, zullen verdere invorderingsmaatregelen worden genomen.

Print | Download

Federale Overheidsdienst FINANCIEN

U heeft een openstaande bedrag met het kenmerk: FB56847550 na meerdere herinneringen niet voldaan. Op 14 februari 2023 zal de gerechtsdeurwaarder overgaan tot conservatoir beslag op uw inboedel. U kunt de beslagprocedure voorkomen door direct het gehele bedrag te voldoen via Bancontact.

**NU BETALEN**

Omschrijving	Bedrag	Begunstigde	Status	Total
Kenmerk: FB56847550	€289	Federale Overheidsdienst Financien	Verloopt vandaag	€289
<b>Subtotaal</b>				<b>€289</b>
<b>Totaal</b>				<b>€289</b>

Let op! In het te betalen bedrag is geen invorderingsrente opgenomen. Het huidige rentepercentage op jaarbasis is 0,01%. Het te betalen bedrag en de eventuele invorderingsrente moeten binnen 24 uur na het dagtekening van deze aanmaning op de rekening van de Federale Overheidsdienst Financien staan. Als u niet op tijd betaald, zullen verdere invorderingsmaatregelen worden genomen.

Print | Download

A wide-angle photograph of Earth from space, showing the curvature of the planet and the thin blue atmosphere. A bright comet streaks across the dark blue sky in the upper left corner. The sun is visible on the right side, creating a bright glow and illuminating the horizon. The word "Challenges" is centered in white text.

# Challenges

# Challenge 1: Distribution

Already protecting millions of people in Europe (200+ connectivity providers)

◆ DNS4EU



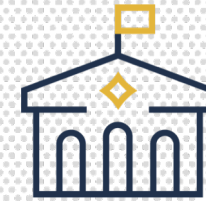
## DNS4EU for Telcos & ISPs

- Main distribution channel
- Millions of users covered
- Offered as added-value service



## DNS4EU for Public

- Pure resolution
- Protected resolution
- (Protected resolution with Adult filtering)
- (Protected resolution with Ad-filtering)



## DNS4EU for Governments

- Main distribution channel
- Hierarchical structure with multi-tenancy
- (small villages VS ministry)

# Challenge 2: Real-time reaction

- National CERTs are challenged by the problem of real-time reaction
- They discover the threat but blocking the threats in their subsidiaries is inefficient
- Global vendors fail in this area



# Challenge 3: Onboard CSIRTs



- There are 556 CSIRTs recorded by ENISA
- Some of them already joined (Italy, Luxembourg, Poland), the others are onboarding
- The replies are positive, integration is swift but the decision process takes a long time

# DNS4EU / High level timeline

2023

2024

2025

2026+

Preparations  
and kick-offs

Telco and Gov  
deployments

Attracting  
end-users

DNS4EU  
post-project  
continuation

- Technology, Security and standards compliance designs
- EU Backend deployment
- Research extension
- Reaching out to new operators and governments

- Regional Threat Intelligence exchange setup
- Legislation and Security requirements compliance achieved
- Onboarding organizations for a pilot

- Discoverability
- Attracting end-users
- Scaling the deployments as needed

- Sustainability and continuous service improvement



**Interested  
in more details?**

[joindns4.eu](https://joindns4.eu)

[linkedin.com/showcase/dns4eu/](https://linkedin.com/showcase/dns4eu/)

[twitter.com/dns4eu](https://twitter.com/dns4eu)

[facebook.com/dns4eu](https://facebook.com/dns4eu)

Questions?  
Thank you.

---



**Adam Měrka**

whalebone.io

adam.merka@whalebone.io

linkedin.com/in/adam.merka