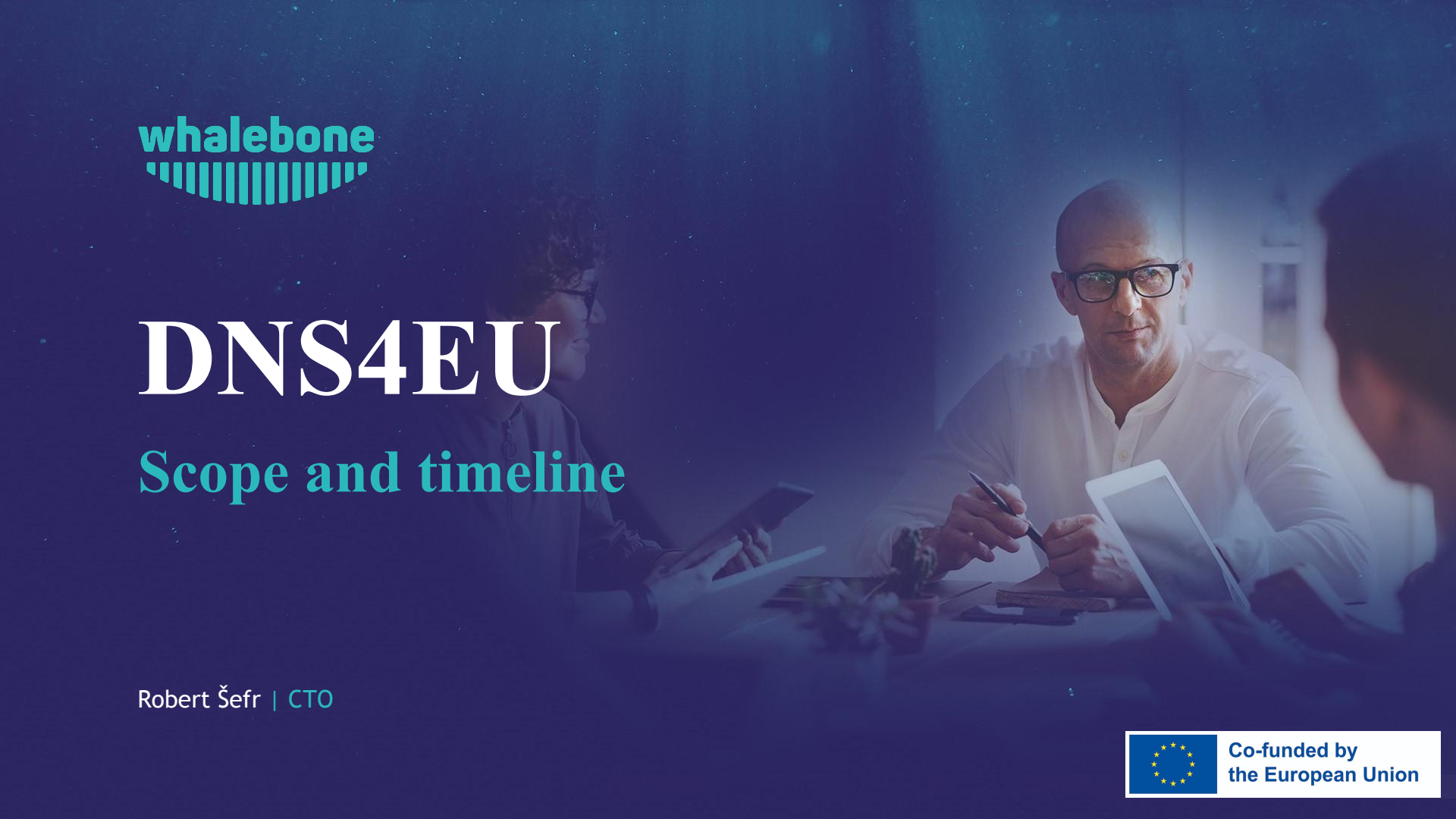
whalebone

DNS4EU

Scope and timeline



Robert Šefr | CTO

Co-funded by the European Union

DNS4EU goals

The goal of DNS4EU is to provide EU citizens, companies, and institutions with a secure, privacy compliant, and powerful recursive DNS. The EU desires to make this the officially recommended DNS resolver for public and governmental institutions.

EU's Digital Sovereignty

The European Commission aims to keep user's data in the Union digital space to support its digital independence and sovereignty.

Onboard 100 Million People

The goal of the DNS4EU is to collaborate with various EU stakeholders to significantly improve the Internet in the EU for many citizens.

Privacy

Citizens of the EU should be provided with DNS resolution that adheres to the highest privacy standards, incl all the EU data privacy regulations.

Security

The consortium combines multiple cybersecurity experts from different EU countries that will work together to provide the safest DNS resolution.

Co-funded by the European Union

DNS4EU Consortium

Consortium Members

- Whalebone, s.r.o. (🇨🇿)
- 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 (🇵🇹)

Co-funded by the European Union

Whalebone overview

Name and date of incorporation
Whalebone, s.r.o.
Incorporated 05/2016
HQ Czech Republic, Brno

Team size
80 (Q3/2023)

Status
Growth, scaling up

Industry
SaaS Network Security, B2B2C(B), B2B, B2G

Customer Segments
Big telcos (Aura; main use case), ISPs (Peacemaker), Corporates & Government (Immunity)

Security problem / opportunity

90% of attacks use an internet domain request – Whalebone blocks access to malicious domains on the DNS level.

Users' sensitive data are often stolen and misused, which can be devastating. Whalebone protects users' identity.

Customers want / expect security from their telecoms and are not receiving it (enough).

Co-funded by the European Union

DNS4EU overview

Threat Intelligence

- Intelligence generated based on the DNS4EU traffic
- Regional intelligence exchange

DNS for Telcos

- On-premise resolver for Telcos
- DNS4EU Threat Intelligence
- (DNS4EU shared IP)

DNS for Governments

- Protective DNS for governments
- DNS4EU Threat Intelligence
- (DNS4EU shared IP)

DNS for end-users

- Public DNS service
- DNS4EU Threat Intelligence
- DNS4EU shared IP

Co-funded by the European Union

Threat Intelligence

Based on DNS4EU traffic

- Actual DNS4EU traffic will be analyzed for new threats and trends
- DNS traffic trends will also be used for false positive mitigation
- Mitigation of global threats
- Tuning the protection accuracy

Regional intelligence exchange

- Setup (or reuse of existing) of platform to exchange the regional Threat Intelligence
- Cooperation with local CERTs/CSIRTs and commercial organizations
- Immediate impact on the DNS4EU resolvers

Co-funded by the European Union

DNS for Telcos

- Telcos are losing control over the traffic and options for optimizations as some users are switching for public DNS providers
- Some end-users may feel lost in the Telco privacy policy or struggle with standard compliance

Telcos

- On-premise DNS resolvers
- National regulatory compliance
- DNS standards support and compliance
- Telco grade resolver including API, monitoring, logging, troubleshooting, and integration features

End-users

- Lower latency than public resolvers
- Transparent privacy policy
- Optional protective features

Co-funded by the European Union

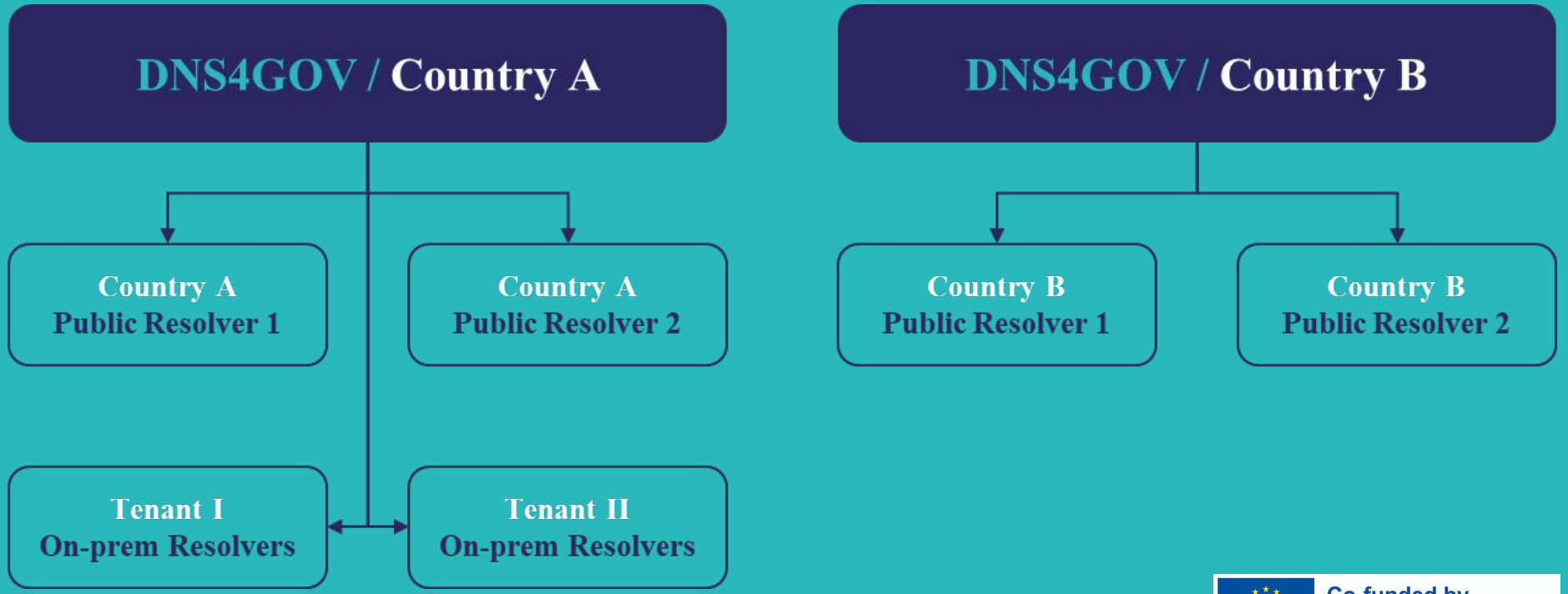
DNS for Governments

- There are many underprotected public organizations (offices, hospitals, schools)
- To fix the issue, governments around the world have started implementing Protective DNS on a countrywide level
- **UK, Australia, Canada** have been running DNS country-wide services for public already for some time, built as turnkey projects
- Rather than a turnkey project, DNS4EU will offer a ready-made product to be deployed (and/or customized) for any region/country

- **Telcos are an ideal partner for B2G sales**

Co-funded by
the European Union

DNS for Governments Architecture



Co-funded by
the European Union

DNS for end-users

- Public and distributed DNS resolvers managed by the consortium members
- Multiple anycast IP addresses / hostnames for different flavours
  - Plain DNS
  - Protective DNS
  - Protective DNS + Adult content blocking
  - …
- Shared IP / hostname with the “DNS for Telcos” if the Telco chooses to do so
- Support for IPv4/IPv6, DNSSec, DNS over TLS, DNS over HTTPS, (DNS over QUIC)

Co-funded by
the European Union

DNS4EU/High level timeline

- Technology, Security and standards compliance designs
- Backend deployment
- Research kick-offs
- Attracting Telcos and Governments

- Regional Threat Intelligence exchange setup
- Legislation and Security requirements compliance achieved

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

- Continuous improvements

Co-funded by the European Union

You and DNS4EU

Let us discuss what DNS4EU can mean for **your** company/institution.

Connect me on LinkedIn

Co-funded by
the European Union

Thank you

Robert Šefr
Whalebone CTO
robert.sefr@whalebone.io

Ondřej Hrabal
Product Marketing Manager
ondrej.hrabal@whalebone.io

Co-funded by
the European Union