

# Team Cymru's Community Services

## UTRS

## LACNOG Webinar

TEAM CYMRU™

**James Shank**

**Chief Architect of Community Services**

TEAM CYMRU

**Founded in 2005**

**Mission:**
**To save and improve lives.**

**We have worked in the background to help stop crime rings, cyber threat actors, and to help protect children and dissidents for many years.**

**We power many major initiatives and well-known vendor offerings.**

**Commercial Services and Community Services**

**Fundado en el 2005**

**Misión:**
**Salvar y mejorar vidas.**

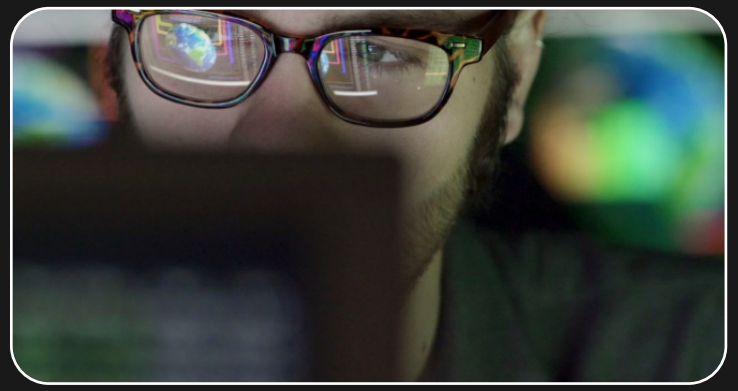
**Hace muchos años que trabajamos en segundo plano para ayudar a detener las redes criminales, los actores de amenazas cibernéticas y para ayudar a proteger a los niños y disidentes.**

**Impulsamos muchas iniciativas importantes y ofertas de proveedores conocidos.**

**Servicios comerciales y servicios comunitarios**

**"Team Cymru pioneered this space. They are the go-to company for leading-edge security teams."**
– John Brown, CISSP, CityLink Telecommunications

# Community Services / Servicios Comunitarios







## Free Tools

- UTRS
- Nimbus
- Malware Hash Registry
- IP to ASN Mapping Service

## CSIRT Assistance

- 124 CSIRT Teams
- 52% of IPV4
- 75% of IPV6

## Restricted Events

- Underground Economy
- Regional Internet Security Events (RISE)

# Free Stuff! / ¡Cosas Gratuitas!

TEAM CYMRU

- Team Cymru provides several services
  - At no cost to you!
  - Some are restricted access (by organization / industry)
  - Some require mutual sharing for access
  - Several are fully free and open

- Team Cymru ofrece varios servicios
  - ¡Sin costo para usted!
  - Algunos son de acceso restringido (por organización o industria)
  - Algunos requieren un intercambio mutuo para acceder
  - Varios son totalmente gratuitos y abiertos

# UTRS

Servico de eliminación de tráfico no deseado

- Como RTBH, pero:
  **upstream** y **global**
- Más de 810 redes participantes
- Reduce el tráfico no deseado que nos afecta a nosotros y a los demás



Unwanted Traffic Removal Service

- Like RTBH, but:
  **upstream** and **global**
- Over 810 participating networks
- Reduces unwanted traffic hitting you and others

# UTRS

TEAM CYMRU



BGP based triggers, with two basic rules:

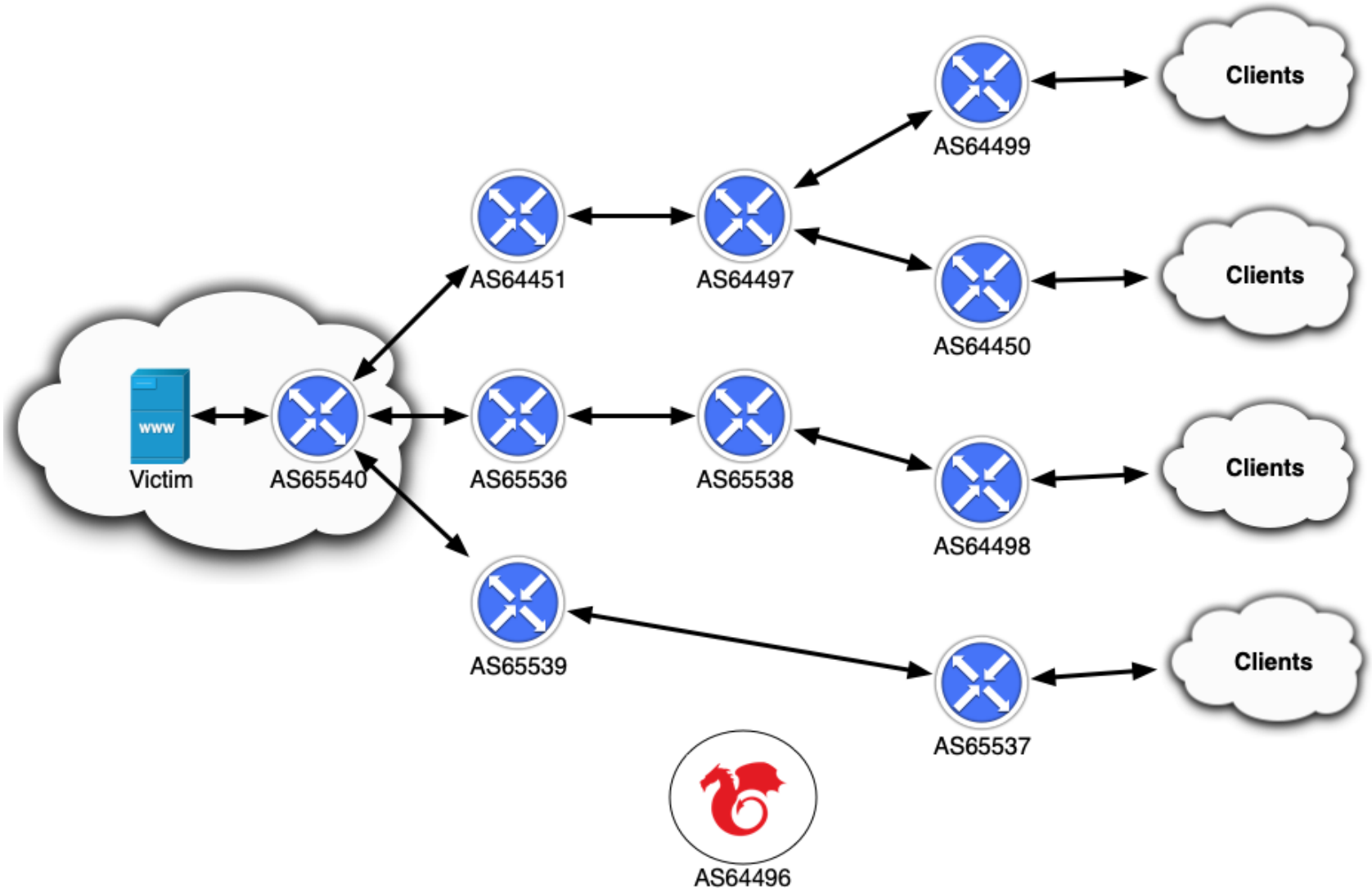
- Accepts only IPv4 /32 advertisements for addresses within prefixes you originate
- You agree to null route traffic to routes received from UTRS

Disparadores basados en BGP, con dos reglas básicas:

- Acepta solo anuncios IPv4 /32 para direcciones dentro de los prefijos que usted origina
- Usted acepta anular el tráfico a las rutas recibidas de UTRS

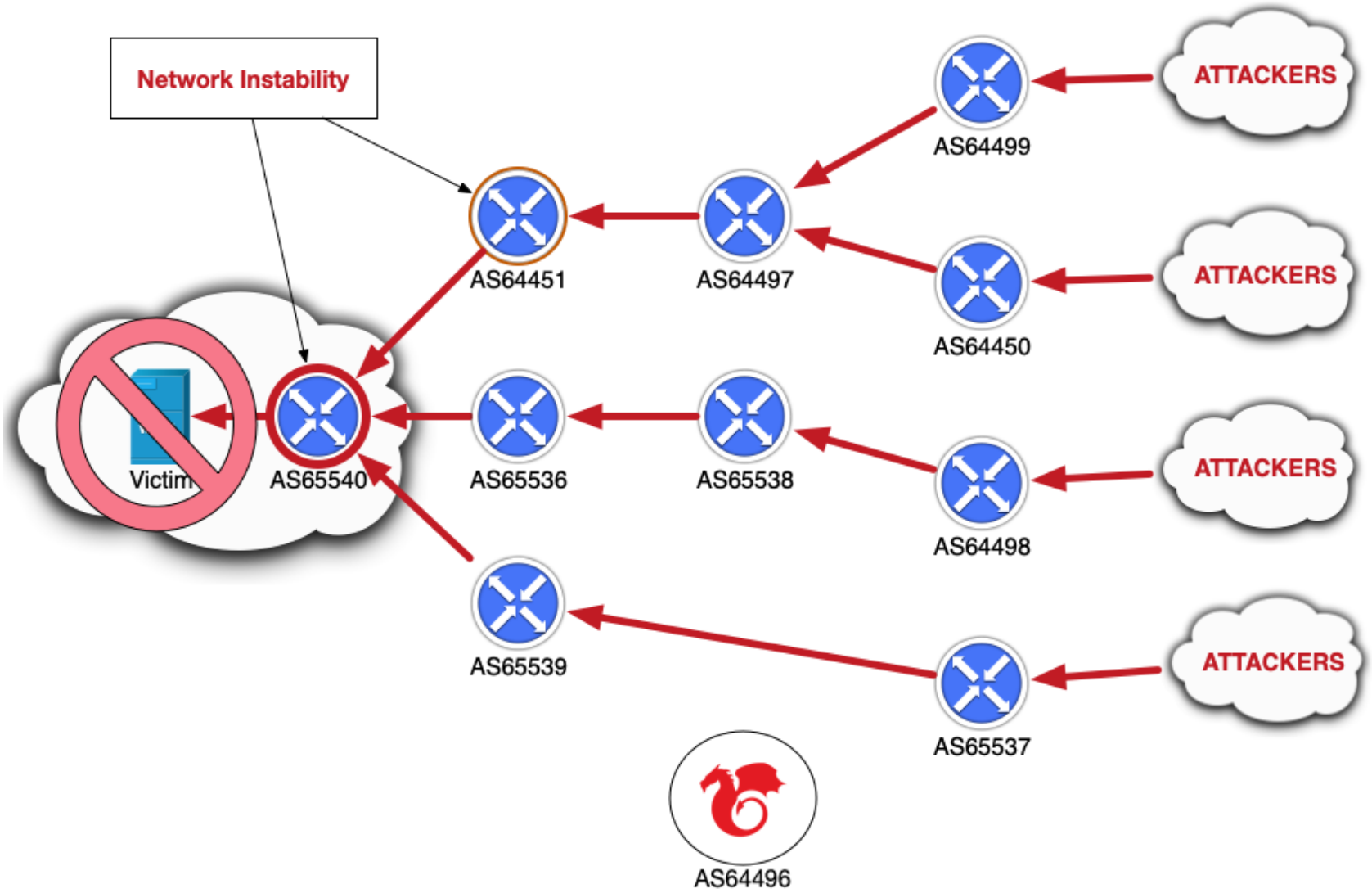
# UTRS

TEAM CYMRU



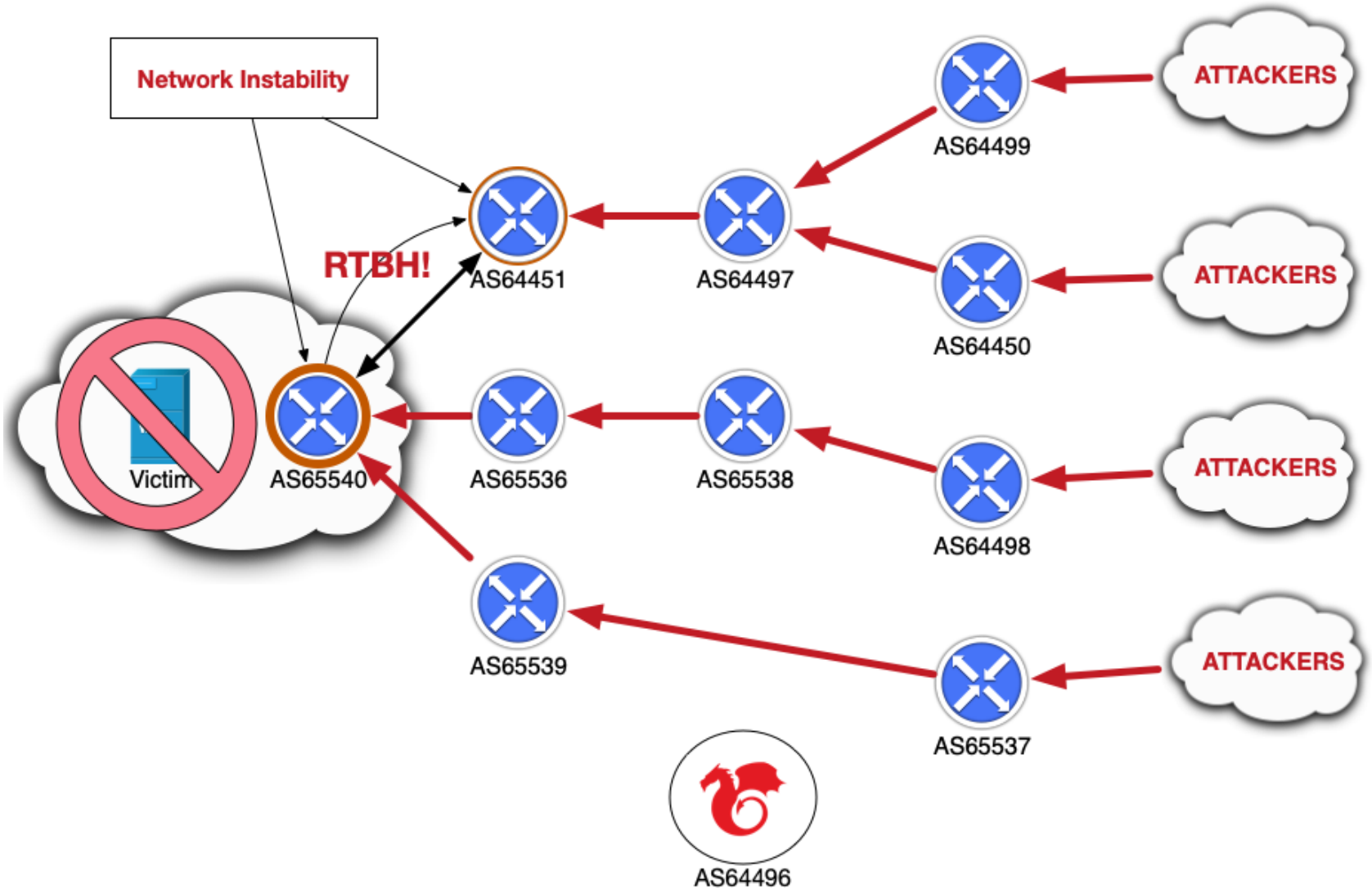
# UTRS

TEAM CYMRU

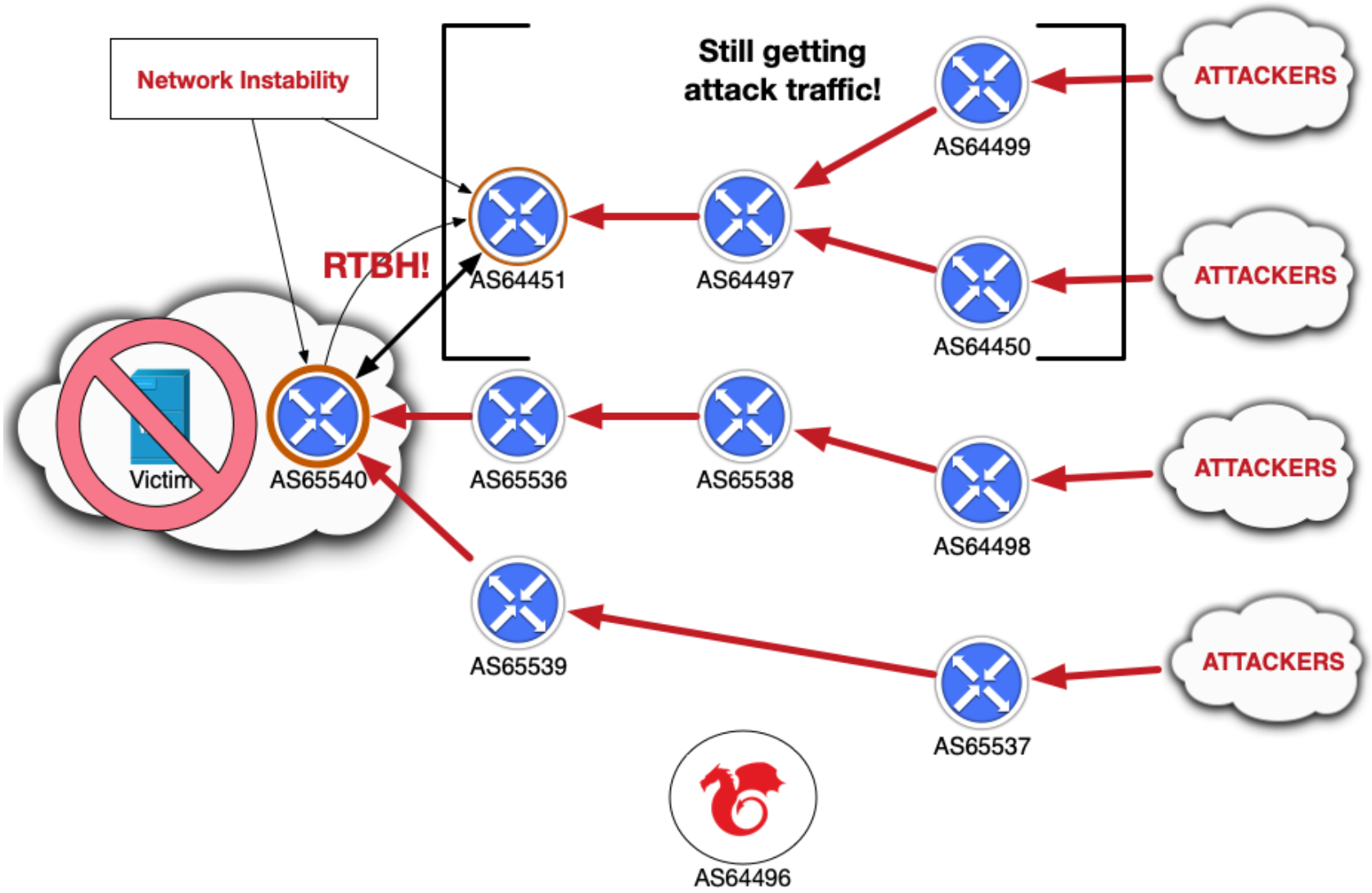


# UTRS

TEAM CYMRU

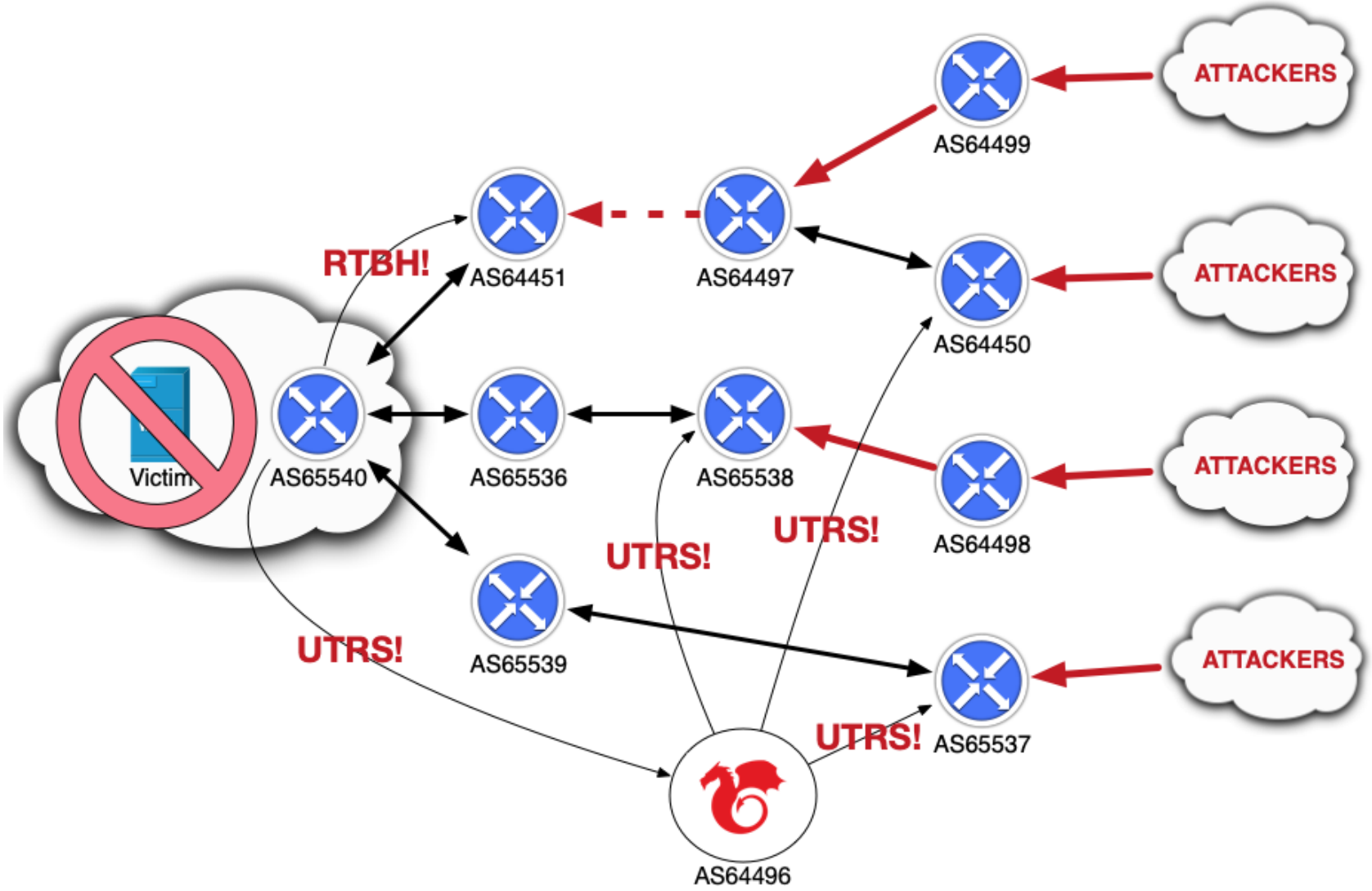


# UTRS


Network Instability
Still getting attack traffic!
RTBH!
Victim
AS65540
AS64451
AS64497
AS64499
AS64450
AS65536
AS65538
AS64498
AS65539
AS65537
AS64496
ATTACKERS
ATTACKERS
ATTACKERS
ATTACKERS

# UTRS

TEAM CYMRU



# UTRS

Consejos para inscribirse:

- El correo electrónico de contacto debe coincidir con el registro del RIR para el AS o la red
- Actualmente solo hacemos peering usando IPv4
- La dirección de peering se debe originar originada desde su AS

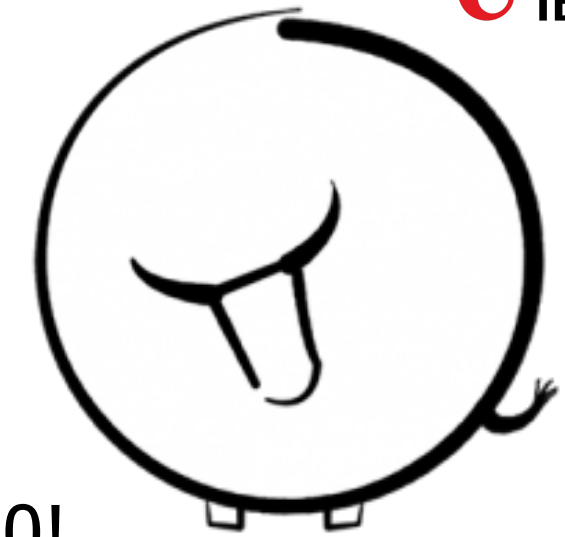


Getting signed up tips!

- Contact email should match RIR's record for AS or network
- We currently only peer over IPv4
- Peering address must be originated by your AS

**https://partners.team-cymru.com/CommunityServices**

# UTRS



How to use UTRS

- Very similar to RTBH
- Add an IPv4 /32 route and advertise it
- Advertise as <YOUR_ASN>:0
- **Remember!** Null route routes from 64496:0!

Cómo usar UTRS:

- Muy similar a RTBH
- Agregue una ruta IPv4 /32 y publíquela
- Anuncie como <SU_ASN>: 0
- **Recuerde:** Descarte el tráfico de las rutas con 64496:0!

**https://partners.team-cymru.com/CommunityServices**

# ¿Preguntas? / Questions?

TEAM CYMRU

Antes de discutir otros servicios, ¿hay alguna pregunta sobre UTRS ahora?



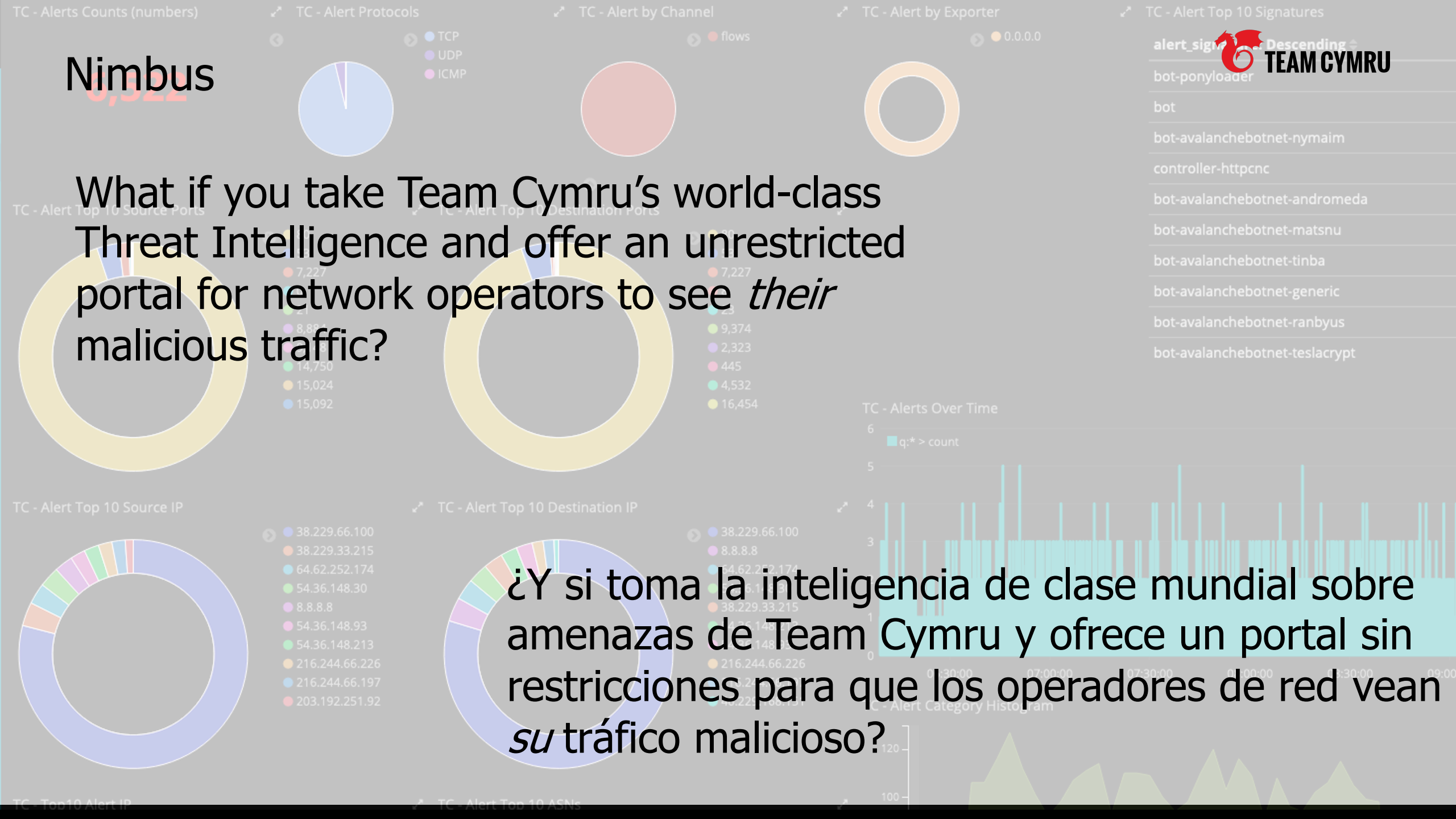
Before discussing other services, are there any questions about UTRS now?

**https://partners.team-cymru.com/CommunityServices**

# Nimbus

What if you take Team Cymru's world-class Threat Intelligence and offer an unrestricted portal for network operators to see *their* malicious traffic?

¿Y si toma la inteligencia de clase mundial sobre amenazas de Team Cymru y ofrece un portal sin restricciones para que los operadores de red vean *su* tráfico malicioso?



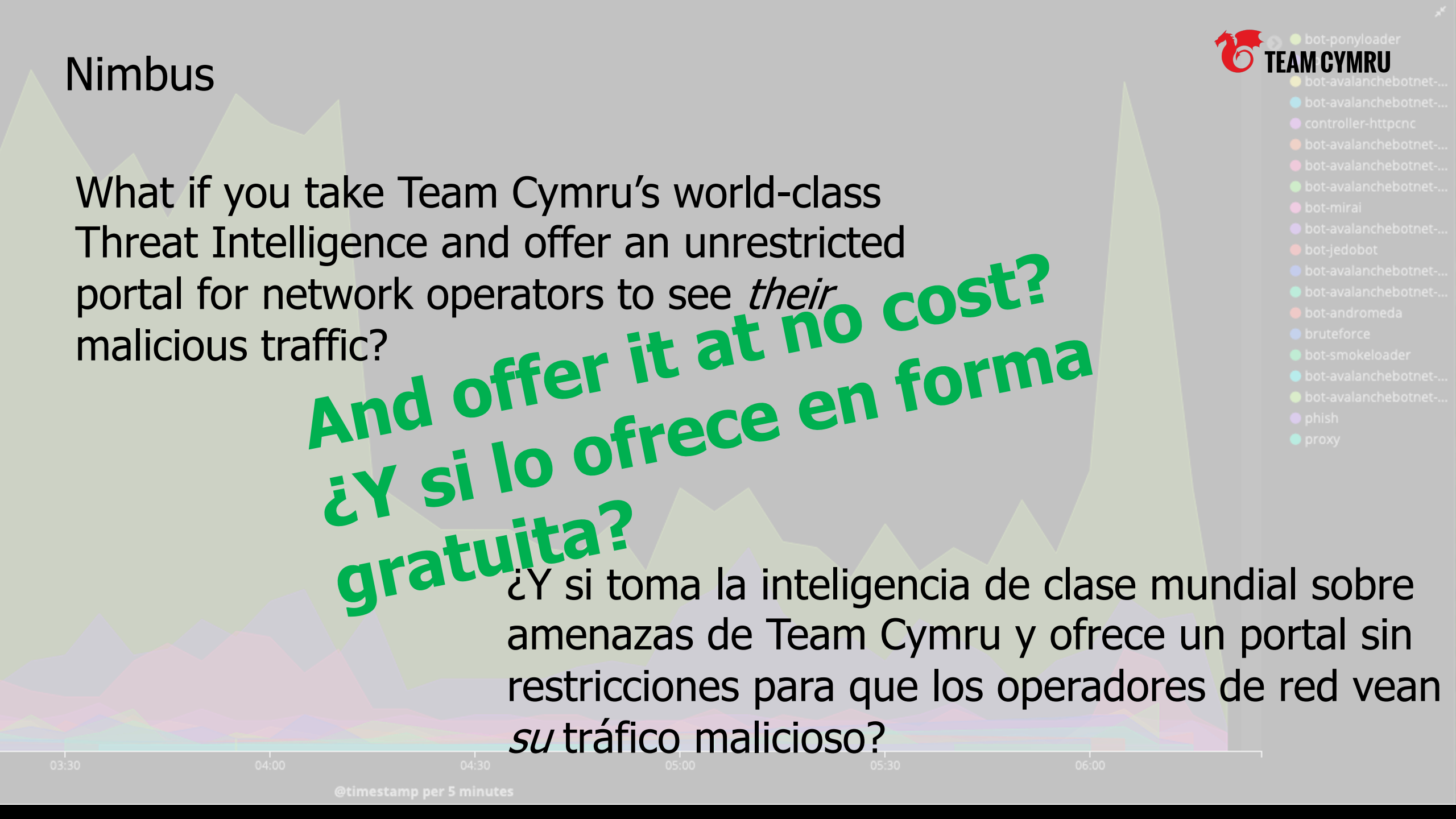
# Nimbus

What if you take Team Cymru's world-class Threat Intelligence and offer an unrestricted portal for network operators to see *their* malicious traffic?

**And offer it at no cost?**

**¿Y si lo ofrece en forma gratuita?**

¿Y si toma la inteligencia de clase mundial sobre amenazas de Team Cymru y ofrece un portal sin restricciones para que los operadores de red vean *su* tráfico malicioso?

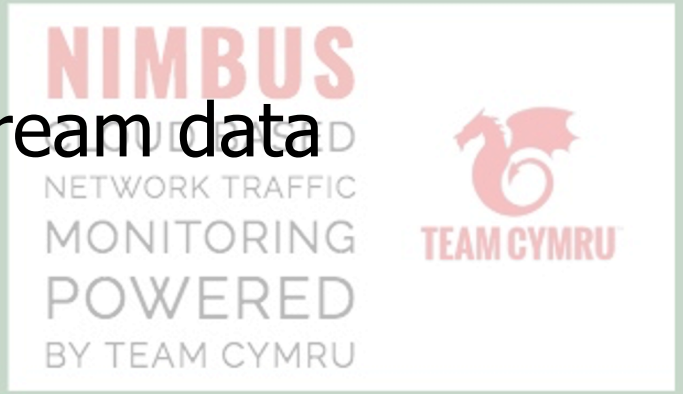


# Nimbus

- Gestionamos el servicio
- Nuestra Inteligencia de amenazas ($ 100.000+ / año)
- Kibana + ElasticSearch
- Su NETFLOW, IPFIX, datos de flujos de red
- Beneficio para la comunidad

- We manage the service
- Our Threat Intelligence ($100,000+/yr feed)
- Kibana + ElasticSearch
- Your netflow, IPFIX, netstream data
- Community Benefit

**https://partners.team-cymru.com/CommunityServices**



# Events

Building bridges between LEOs and InfoSec Pros

- 20% - 35% LEOs, 50% InfoSec Pros, 15% Financial, some academia + industry
- Vetted and trusted, TLP:RED talks

Construyendo puentes entre los LEO y los profesionales de la seguridad de la información

- 20% - 35% LEOs, 50% profesionales de infosec, 15% sector financiero, algo sector académico + industria
- Validado y confiable, conversaciones TLP:RED

# Economía Subterránea

- Suele tener lugar en Europa a principios de septiembre (con cambios este año debido al COVID-19)
- Coanfitriones anteriores: Interpol, Europol, Consejo de Europa, Qatar MOI, Banco La Caixa, CERT-UK, RoEduNet (Rumania)



- Usually takes place in Europe in early September (COVID-19 changes this year)
- Past CoHosts: Interpol, Europol, Council of Europe, Qatar MOI, La Caixa Bank, CERT-UK, RoEduNet (Romania)

# RISE



TEAM CYMRU

Regional Internet Security Events

- Three per year
- Smaller, 100 – 250 people
- Past six: Uruguay, Kenya, Brazil, Hong Kong, USA, Finland (Colombia May 2020 cancelled)
- Future: TBD, but will resume when safe
- Interested in hosting? outreach@cymru.com

Eventos regionales de seguridad en Internet

- Tres por año
- Más pequeños, 100 - 250 personas.
- Últimos seis: Uruguay, Kenia, Brasil, Hong Kong, EE. UU., Finlandia (Colombia mayo de 2020 se canceló)
- Futuro: TBD, pero se reanudarán cuando sea seguro
- ¿Le interesaría albergar uno de estos eventos? outreach@cymru.com

# Event Sponsors / Patrocinadores de los eventos



# CAP

TEAM CYMRU



CSIRT Assistance Program (CAP)

- Free reputation data
- Contains our filtered set of threat intelligence
  - Specific to “jurisdiction”
- Available to Regional and National CSIRTs only

Programa de asistencia CSIRT (CAP)

- Datos de reputación gratis
- Contiene nuestro conjunto filtrado de inteligencia de amenazas
  - Específico para cada “jurisdicción”
- Disponible solo para CSIRT regionales y nacionales

# Other Services

- IP to ASN Mapping:
  https://team-cymru.com/community-services/ip-asn-mapping/
- Malware Hash Registry:
  https://team-cymru.com/community-services/mhr/
- Dragon News Bytes:
  https://team-cymru.com/community-services/dnb/

# Thank You! ¡Gracias!



TEAM CYMRU

Be part of our community!

¡Únase a nuestra comunidad!

**OUTREACH@CYMRU.COM**

For questions about anything discussed today…

Si tiene alguna pregunta sobre cualquiera de las cosas que discutimos hoy ...

**JSHANK@CYMRU.COM**



# Thank you.
# ¡Gracias!

CYMRU.COM | 847-378-3300
© 2020 TEAM CYMRU, INC. ALL RIGHTS RESERVED.