

TICAL 2023

# pDNSSOC

## Fortaleciendo la Seguridad en el sector de Investigación y Educación

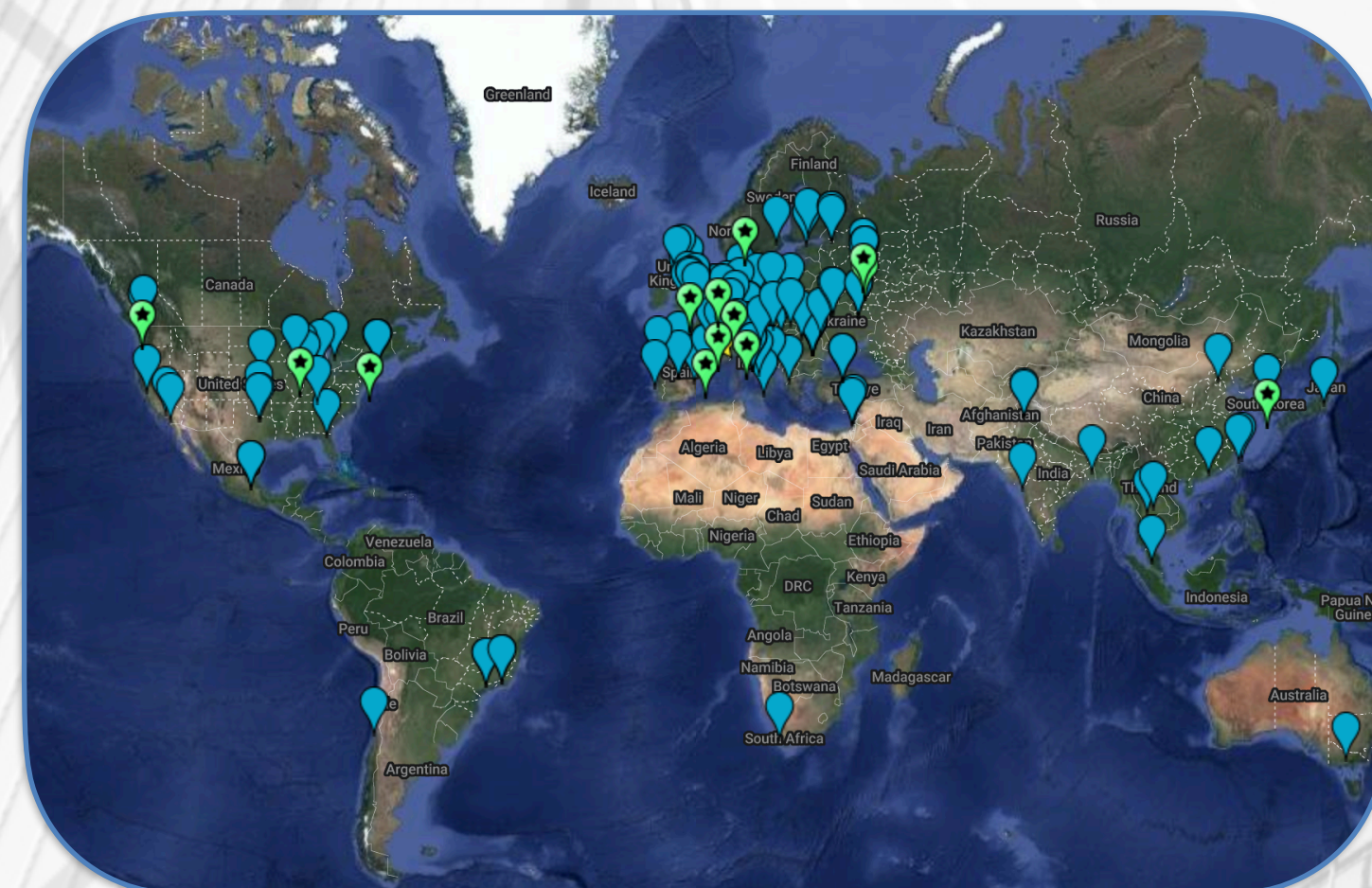
Pau Cutrina / CERN



**TLP:CLEAR**

# [pau.cutrina@cern.ch]\$ whoami

- Coordino la **respuesta de incidentes** del **grid de computación** del CERN
  - 611 organizaciones de 42 países con +1M CPUs y 1EB storage
- Contribuyo activamente a la investigación y **persecución de criminales**
- Mi objetivo es posicionar a **RedClara** en el **centro de la red de inteligencia global**



# Operation Windigo (Ebury)

- WLCG fue la principal víctima durante 3+ años
- **+1.500 organizaciones** de educación e investigación

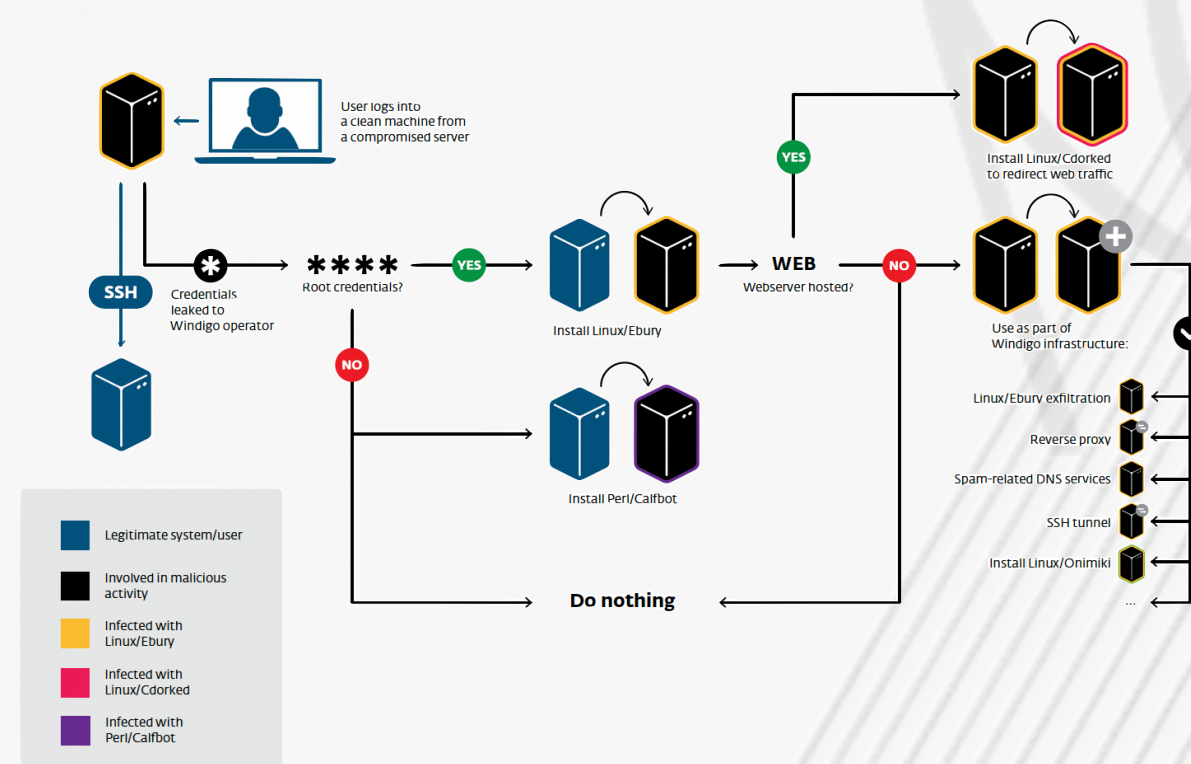
## OPERATION WINDIGO

The vivisection of a large Linux server-side credential stealing malware campaign

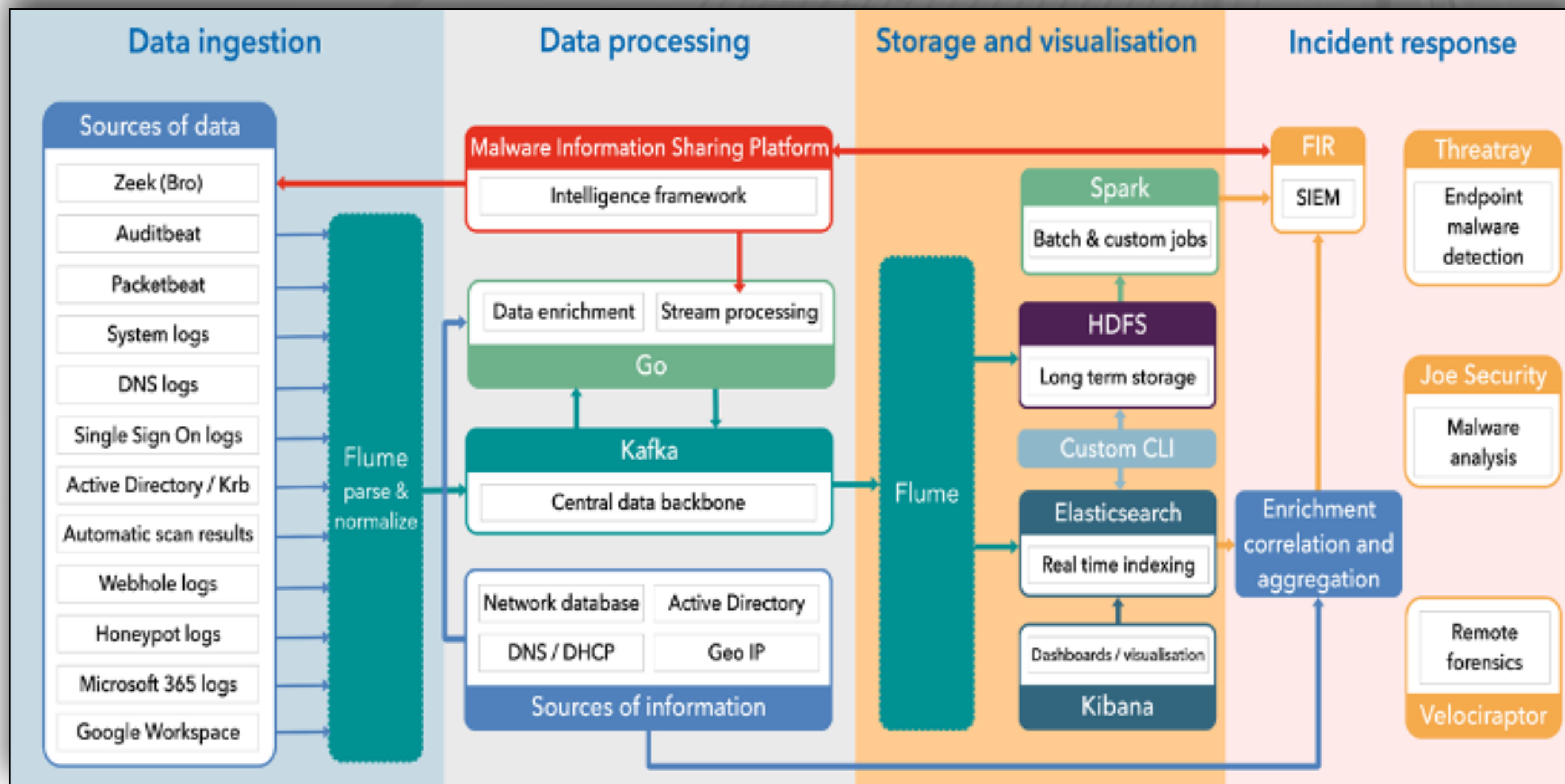


### Key Findings

- The Windigo operation has been ongoing since at least 2011
- More than **25,000 unique servers have been compromised** in the last two years
- A wide range of operating systems have been compromised by the attackers; Apple OS X, OpenBSD, FreeBSD, Microsoft Windows (through Cygwin) and Linux, including Linux on the ARM architecture
- Malicious modules used in Operation Windigo are designed to be portable. The spam-sending module has been seen running on all kinds of operating systems while the SSH backdoor has been witnessed both on Linux and FreeBSD servers
- Well known organizations including cPanel and Linux Foundation fell victim of this operation
- Windigo is responsible for sending an average of **35 million spam messages on a daily basis**
- More than 700 web servers are currently redirecting visitors to malicious content
- Over half a million visitors to legitimate websites hosted on servers compromised by Windigo



# CERN SOC



# ¿Qué es Threat Intelligence (TI)?

- Definir las **amenazas** dirigidas a una organización
- Comprender los **comportamientos** de los atacantes

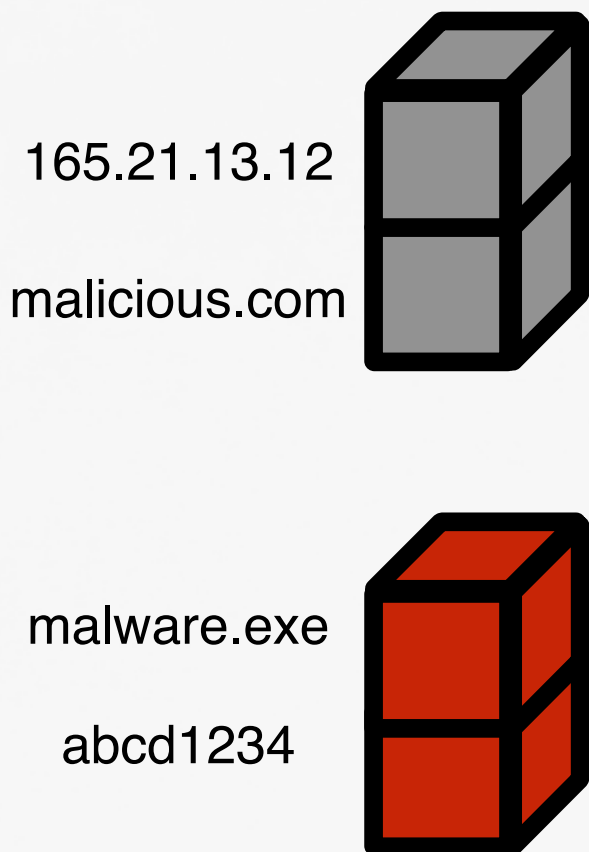
## Objetivos

- Tomar **decisiones** más rápidas e informadas
- **Detectar y responder** a las amenazas

# Threat Intelligence (TI)

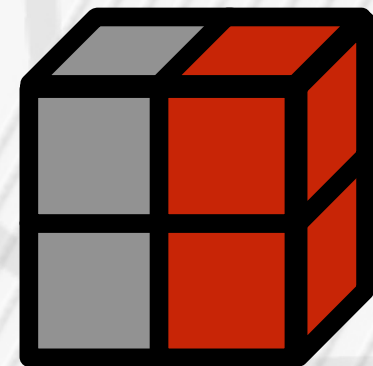
## Detección

Dominio: **malicious.com**  
IP: **86.105.245.69**  
Nombre: **malware.exe**  
Hash: **abcd1234**



## Análisis

**malware.exe** es un archivo con el hash **abcd1234** y exfiltra datos a **86.105.245.69** desde el 1-Oct-23



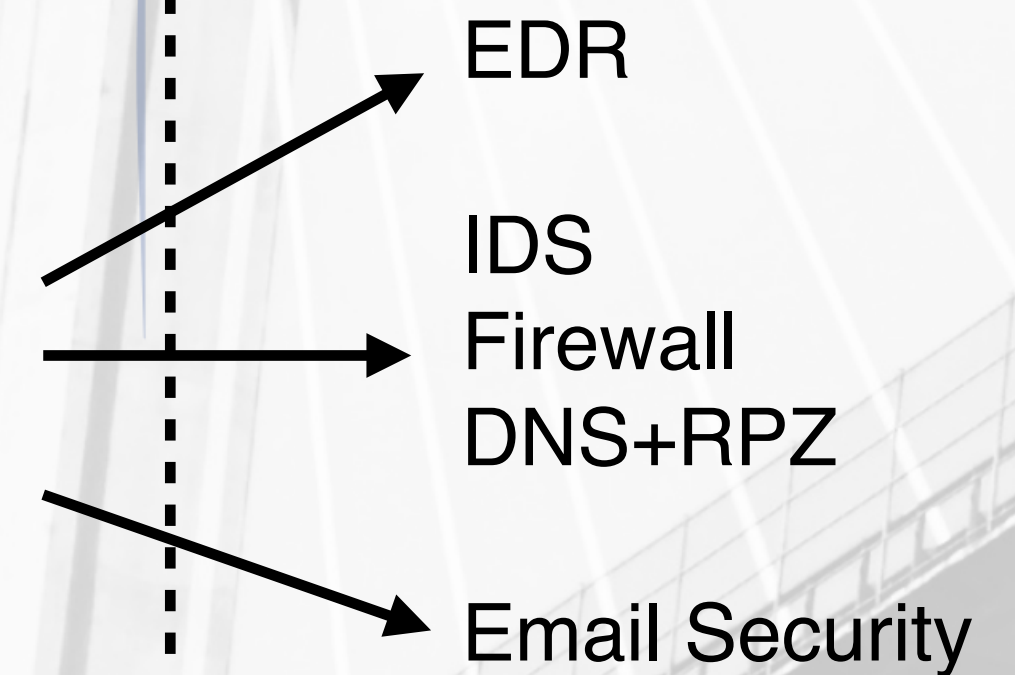
## Inteligencia

El **grupo XYZ** tiene como objetivo **R&E** y despliega **ransomware**



## Respuesta

Buscar y eliminar el malware, bloquear las IPs, blacklist dominio



# MISP

- **Agrupar** inteligencia
  - IOCs gratuitos o comerciales
  - IPs, dominios, hashes, ...
- **Distribuir** con otras instancias de MISP
  - Específicas del sector
  - Gobierno
  - Entidades privadas

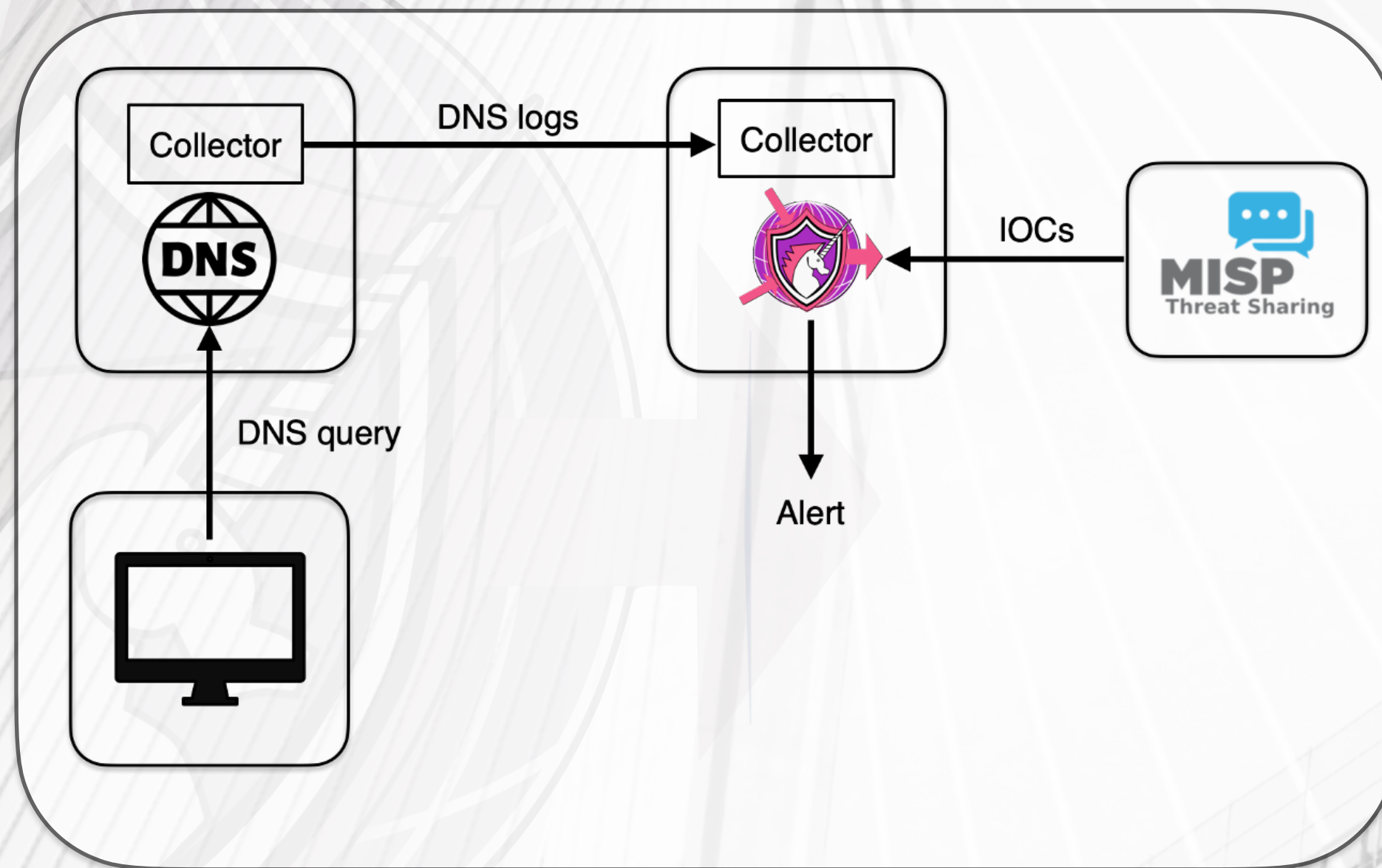
The screenshot displays the MISP interface for an event titled "Emotet campaign used to deploy Ransomware". The event ID is 33098, and it is associated with the CERN organization. The event is in unprotected mode and has a high threat level. It includes tags for Ransomware, emotet, PAP:AMBER, and ip:amber. The event was recorded on 2023-11-07. The interface shows a list of related events and a table of attributes.

Date	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS
2023-11-07	Payload delivery	filename	malware.exe			malware.exe is the emotet payload use dto connect to the C2. Detected by the EDR.	✓	892 5435		
2023-11-07	Network activity	ip-dst	86.105.245.69			IP used to exfiltrate data. It resolves the domain malicious.com. Detected on the IDS, DNS and firewall.	✓			
2023-11-07	Network activity	domain	malicious.com			Domain used to exfiltrate data. Detected on the DNS logs.	✓			✓

# pDNSSOC



1. Envío de la query **contextualizada**
2. **Correlación** de IP y dominio
3. **Notificación**

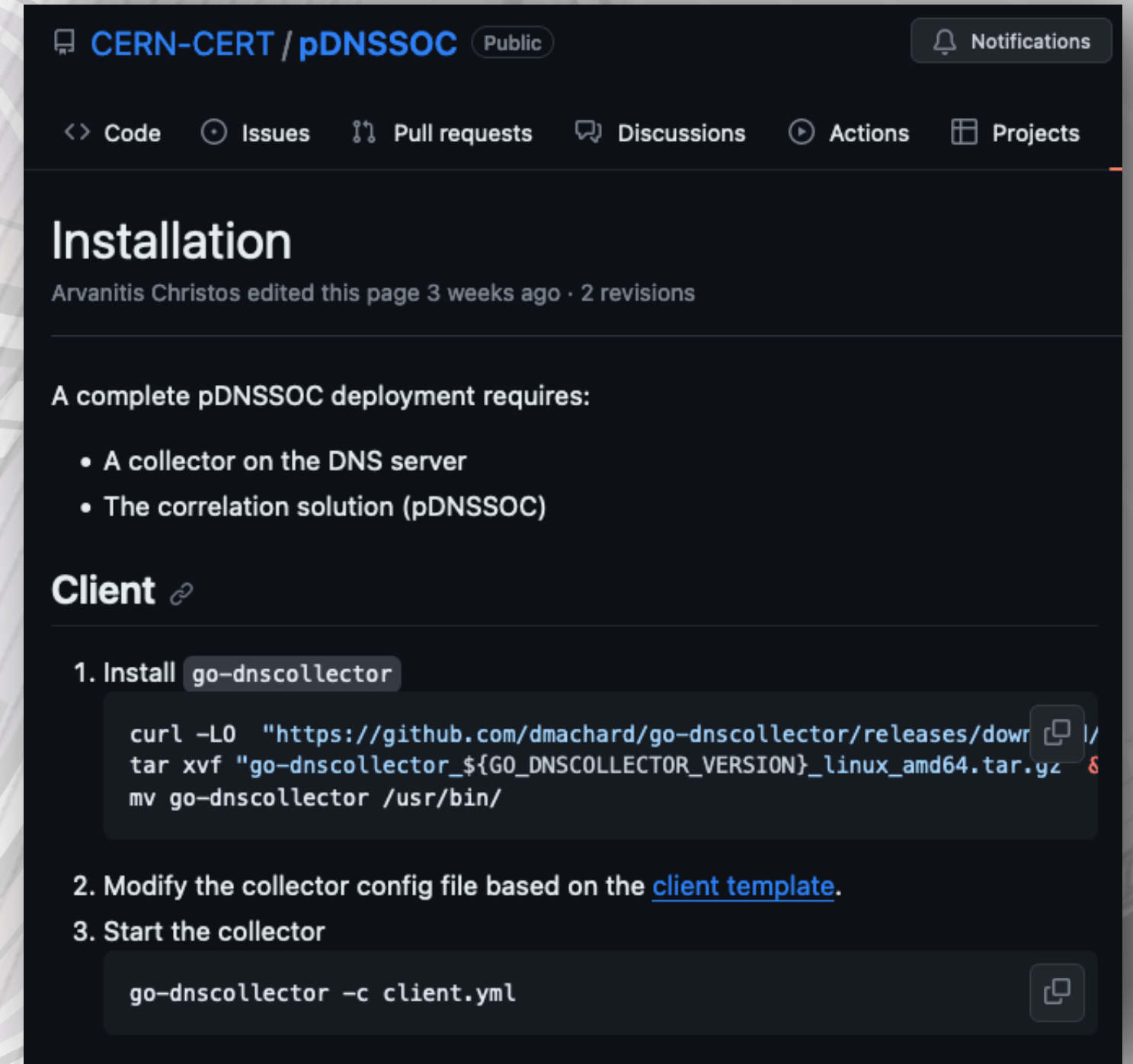


*Recopilar registros de DNS y convertir la inteligencia en alertas*



# Visión general

- Proyecto de **código abierto**
- **Mínimos recursos** necesarios
  - +60 hospitales: < 2 vCPU, 2Gb RAM, 10Gb
- **Configuración rápida y sencilla**
  - < 5min
- Mínimas intervenciones en el servidor DNS



CERN-CERT / pDNSSOC Public

Code Issues Pull requests Discussions Actions Projects

## Installation

Arvanitis Christos edited this page 3 weeks ago · 2 revisions

A complete pDNSSOC deployment requires:

- A collector on the DNS server
- The correlation solution (pDNSSOC)

### Client

1. Install go-dnscollector

```
curl -LO "https://github.com/dmachard/go-dnscollector/releases/download/v1.0.0/go-dnscollector_${GO_DNSCOLLECTOR_VERSION}_linux_amd64.tar.gz" &
tar xvf "go-dnscollector_${GO_DNSCOLLECTOR_VERSION}_linux_amd64.tar.gz" &
mv go-dnscollector /usr/bin/
```
2. Modify the collector config file based on the [client template](#).
3. Start the collector

```
go-dnscollector -c client.yml
```

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

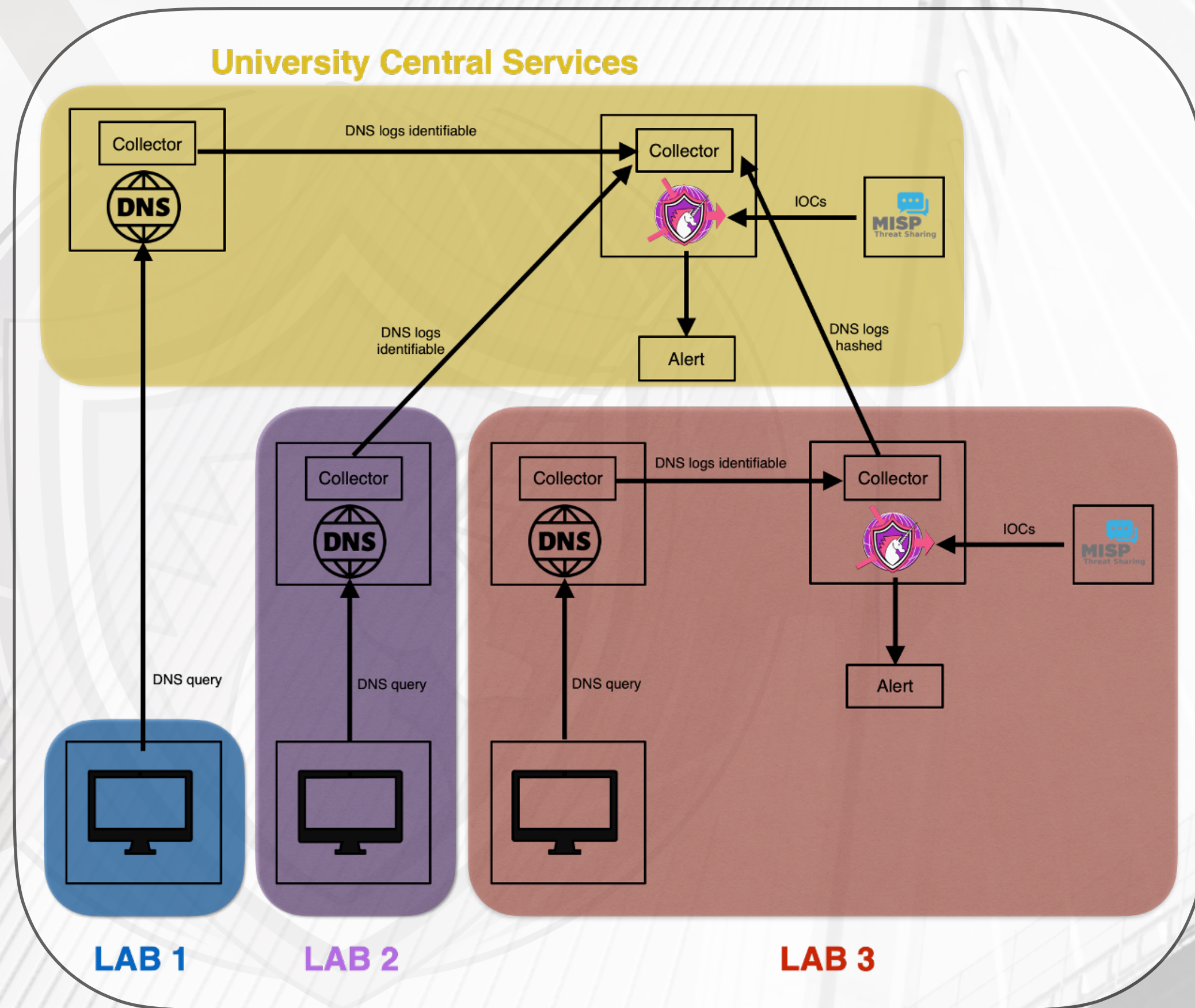
# Objetivos

- Integrar la **inteligencia** como valor central de la seguridad
- **Difusión** inmediata de la información
- Responder como una **comunidad** global
- Respetar la **confidencialidad** (TLP)
- Respetar la **privacidad** de los usuarios



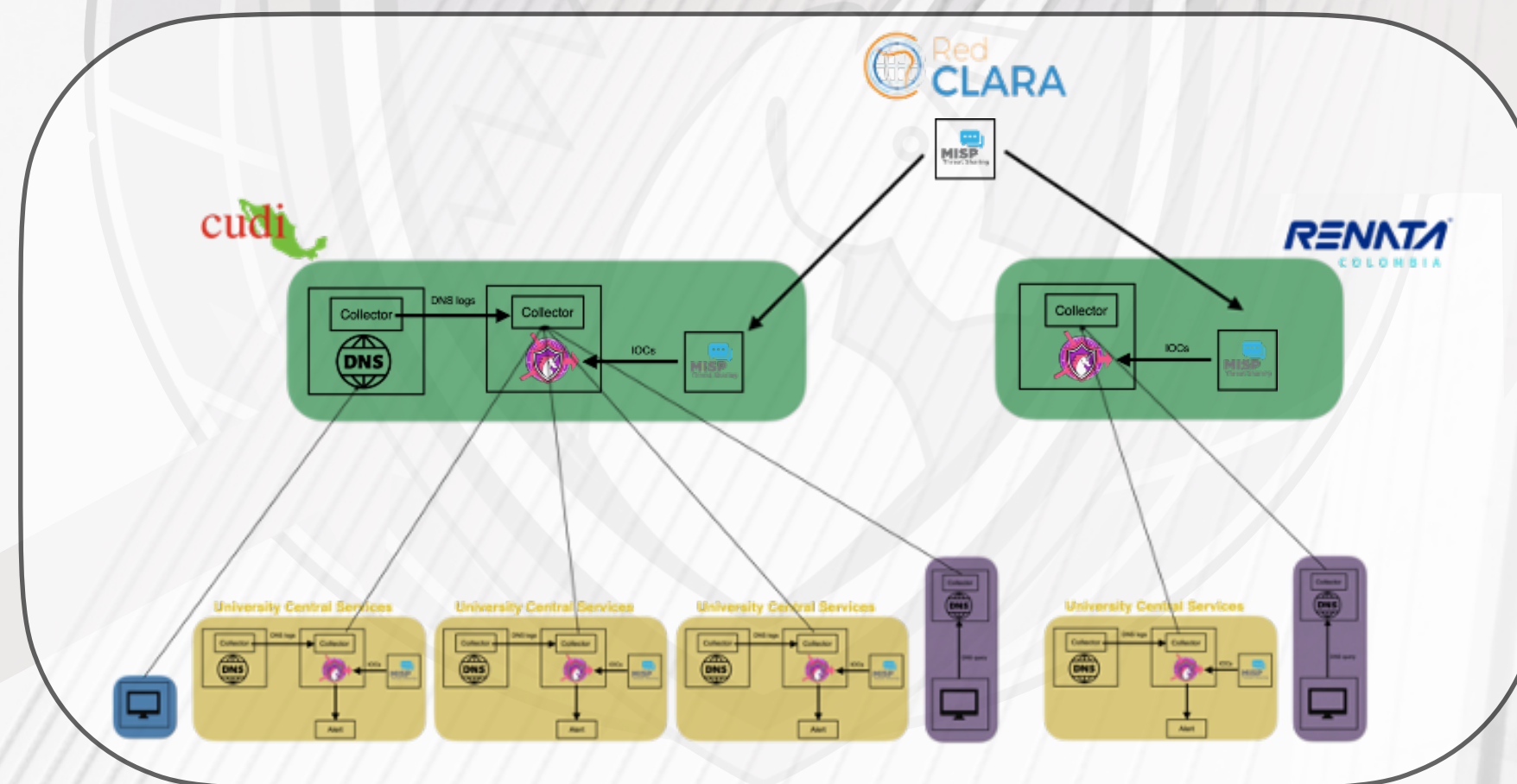
*Abriendo las puertas a la detección y correlación de incidentes  
a **todas las organizaciones** usando inteligencia de calidad*

# Modelos de Implementación



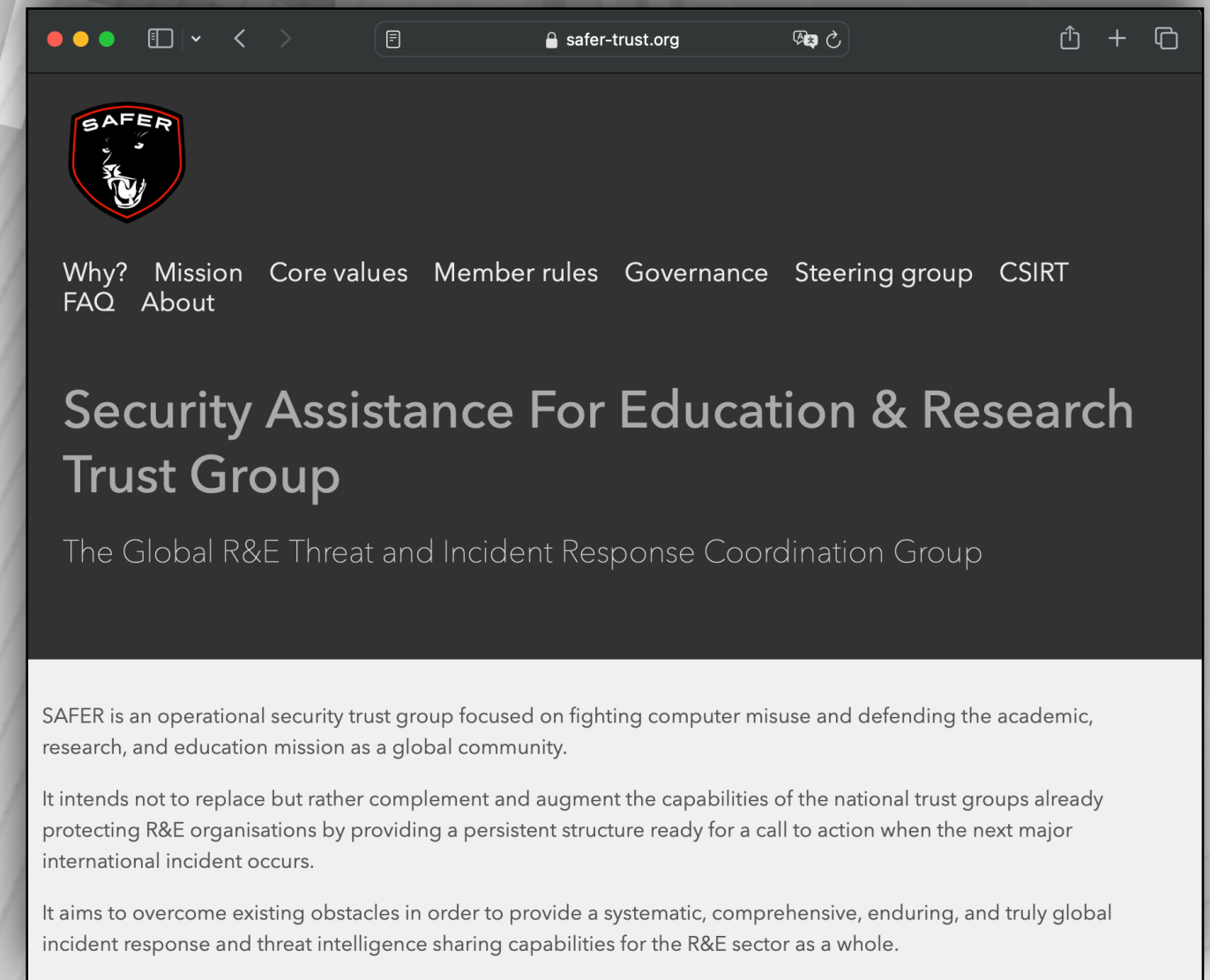
# Pasos a seguir

1. **Definir modelo y recursos** disponibles.
2. Despliegue de la **infraestructura y configuración** de las herramientas
3. Definición de **políticas, procedimientos y estrategia**



# SAFER

- **Alcance global**
- Sin importar el país de origen o la financiación
- **Independiente**
- Impulsado y mantenido por los **miembros**
- **Conectar** grupos de seguridad existentes

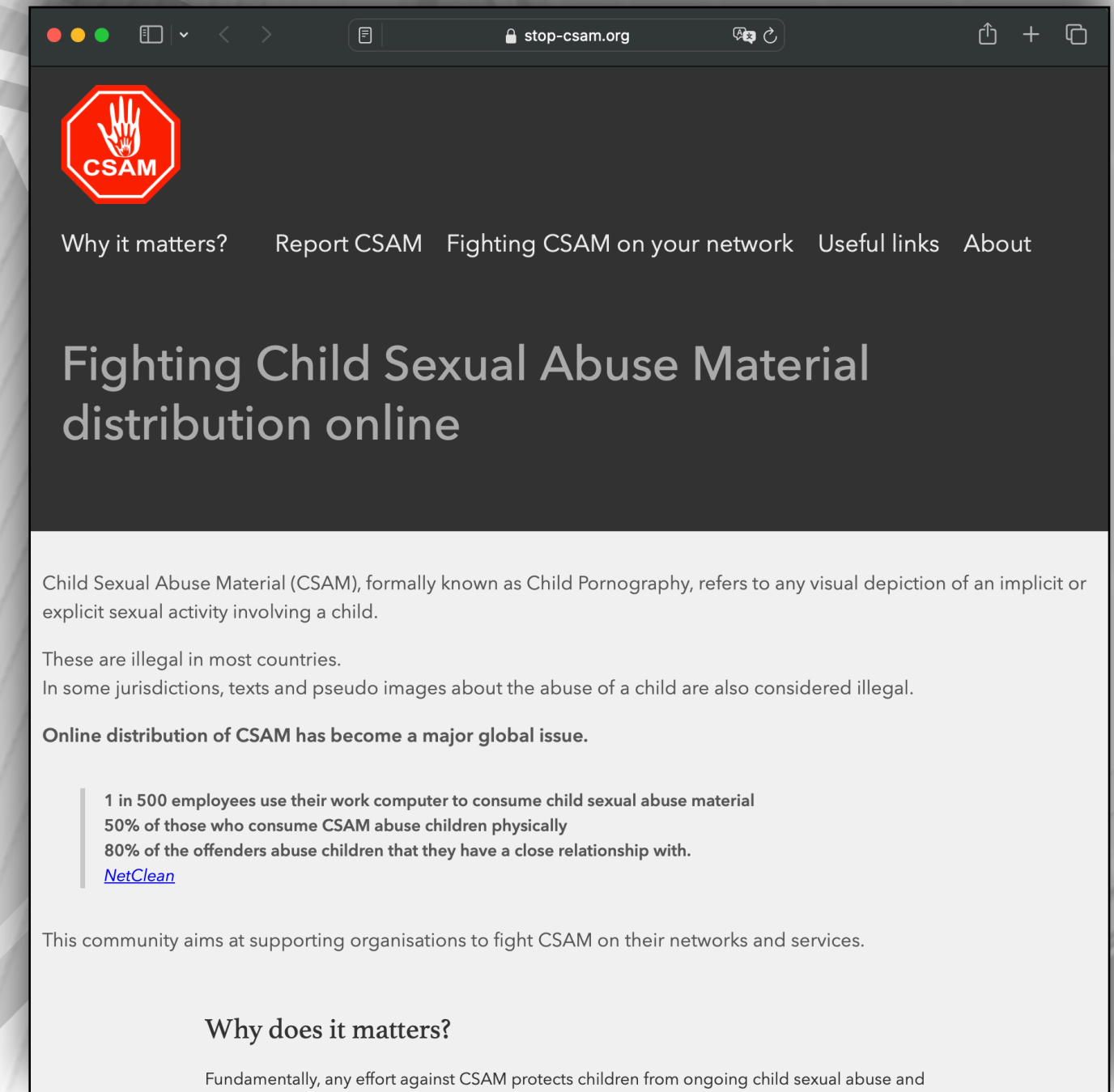


<https://safer-trust.org>



# Motivación

1. Proteger **infraestructura crítica** y sus **usuarios**
2. Implementar **estrategias** de respuesta globales
3. Frenar la **ciberdelincuencia**



<https://stop-csam.org>

# Futuro

- Que el **intercambio de inteligencia** sea una prioridad principal
- Trabajar juntos **compartiendo recursos** sea una práctica común
- Que la **colaboración** en respuesta a incidentes sea parte de los procedimientos

***Conectados por redes, unidos por seguridad***

Red  
**CLARA**



**TICAL**  
Comunidad y tecnología



# Agradecimientos

*Agradecimiento especial a **TICAL** por la amable invitación, así como a **Carlos** de RedClara y a **Moisés** y **Fernando** de CUDI por su valiosa colaboración y contribución a nuestra comunidad*

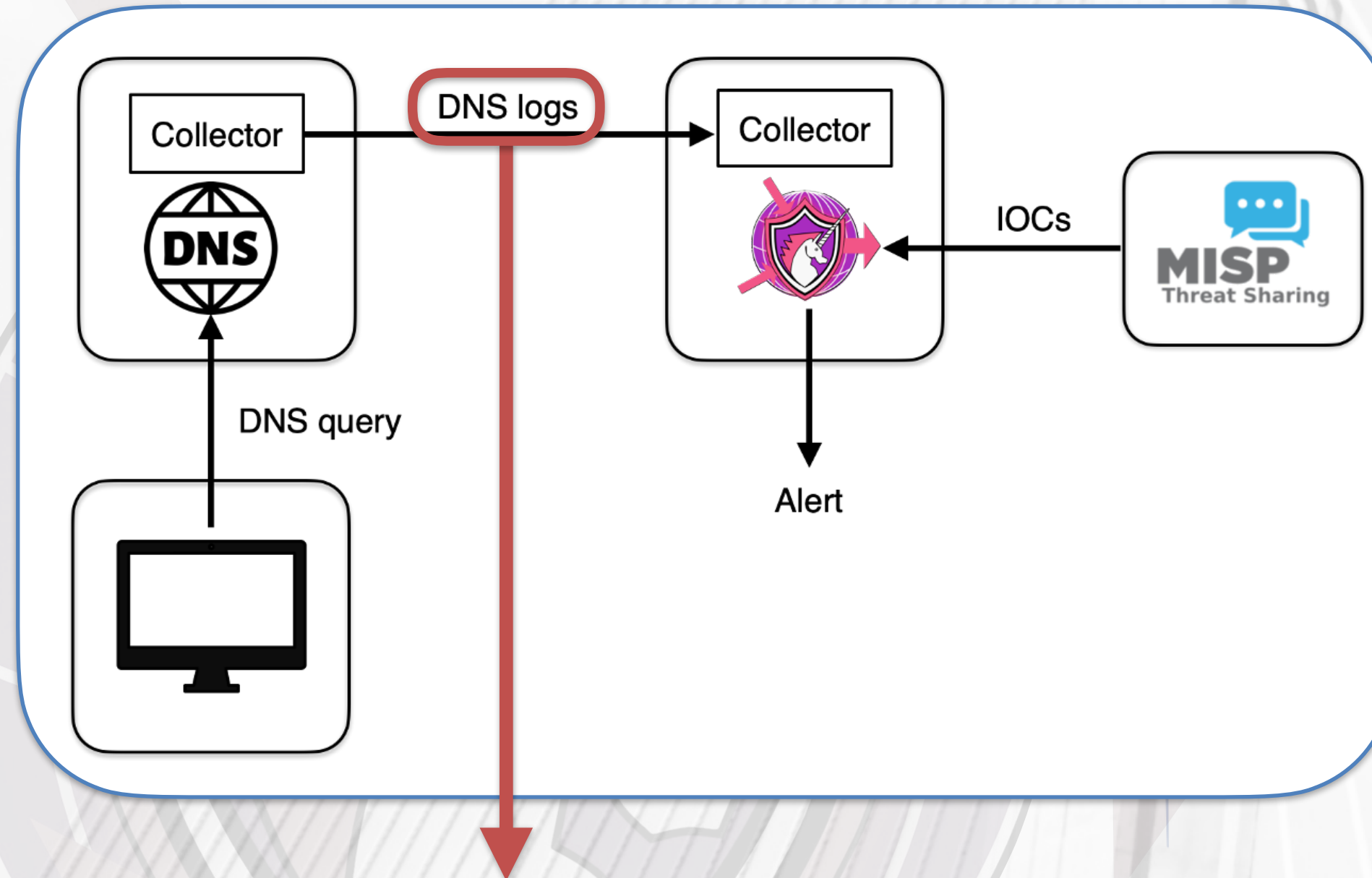


# ¡GRACIAS!

Pau.Cutrina@cern.ch



# Privacidad



Non Anonymized: {"response-ip":"137.43.124.55","qname":"malicious.com", "query-ip":"188.184.10.32"...}

Hashed: {"response-ip":"137.43.124.55","qname":"malicious.com", "query-hash":"52293267a91b9fb=" ...}

Pointer: {"response-ip":"137.43.124.55","qname":"malicious.com", "sensor-id":"CERN\_DNS\_01"...}

Anonymized: {"response-ip":"137.43.124.55","qname":"malicious.com", ...}

# DNSTAP

```
26-Oct-2023 16:32:12.081 client
@0x7fbb3e321480 185.80.*.*#36851 (example.com):
query: example.com IN TYPE65 + (DNS_SERVER_IP)
```

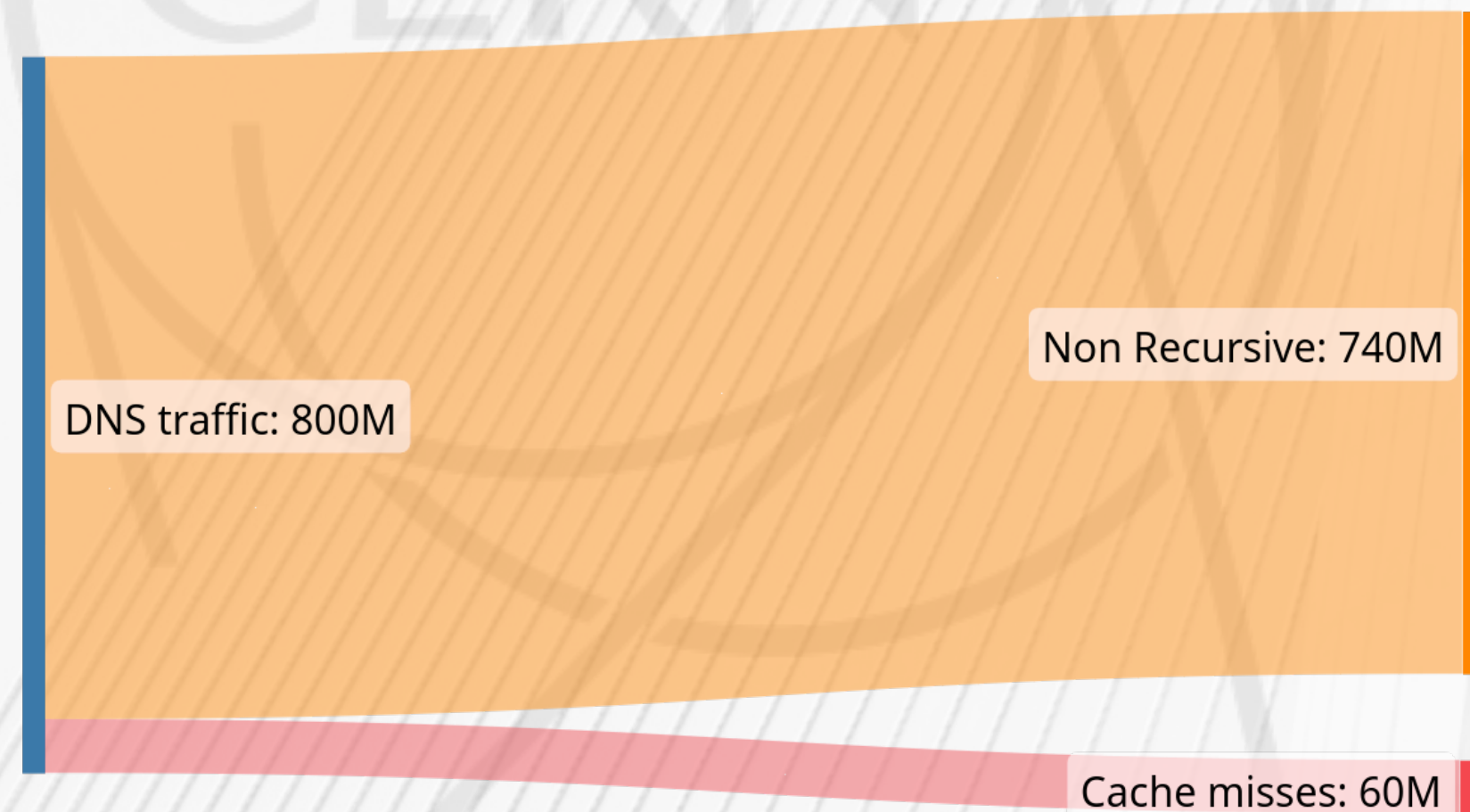
## Server Query Logs

```
{
  "family": "IPv4", "protocol": "UDP",
  "query-ip": "188.184.*.*", "query-port": "56537",
  "response-ip": "50.116.16.111",
  "dns": {
    "rcode": "NOERROR", "qname": "malicious.top",
    "qtype": "A",
    "flags": {
      "qr": true, # Response to query
      "aa": true, # Authoritative Answer
    },
  },
  "resource-records": {
    "an": [{ "name": "malicious.top", "rdatatype": "A",
      "ttl": 60, "rdata": "50.116.16.111"}],
  },
},
"operation": "CLIENT_RESPONSE", "identity": "dnstap_client",
"timestamp-rfc3339ns": "2023-09-10T20:16:18.913238827Z",
}
```

## DNSTAP Logs

# DNS data

- Procesar solo el tráfico por encima del recursivo (no encontrados en caché) resulta en una cantidad significativamente menor de datos.
- En CERN, los no encontrados en caché representan el 5% del tráfico DNS total.



# Falsos Positivos

- Ajustar el filtro de IOCs en MISP
  - Warning Lists
  - to\_ids
- Definir intervalos de tiempo para las taxonomías

```
# pdnssoc-cli configuration
periods:
  generic: # Take into account only attributes that have been published for the past month
    delta:
      days: 30
tags:
- names:
  - "APT" # Fetch all APT tagged without time restrictions
```

# Modelos de Implementación

